12 February 2025

Comments of

ACT | The App Association

to the

United Kingdom's Competition and Markets Authority (CMA)

regarding its

Strategic Market Status Investigations into Apple's and Google's mobile ecosystems

Introduction and statement of interest

ACT | The App Association is a trade association representing small business technology companies from across the United Kingdom (UK), European Union (EU), and the United States (U.S.). 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.

Small and Medium-Sized Enterprises (SMEs) are a key engine of the UK technology economy

The UK has the third largest tech sector in the world, valued at more than $1.2 trillion. In 2021, 56 per cent of the digital sector's £182.1 billion gross value add contribution to the UK economy came from SMEs. SMEs account for more than 50 per cent of all private sector jobs in the UK.[1]

The small business-driven app economy is vital to UK prosperity

A huge amount of economic activity involves mobile apps, much of which we do every day without a second thought. A few examples include shopping, booking travel, gaming, banking, watching media, working, communicating, teaching kids in school, monitoring our health, and learning new languages. Apps are also used to control our homes, cars, factories, and medical devices, plus countless more activities, via the internet of things (IoT). These activities don't just generate money; they increase sustainability, boost productivity, and provide critical support to countless consumers and businesses.

The term we use for this broad ecosystem of economic benefit is 'the app economy', and it is a significant contributor to the UK's financial success. The direct revenues of the UK app economy in 2021 amounted to £33 billion. Including direct and indirect contributions, the app economy generated £74.8 billion in revenue throughout all sectors of the UK's economy in 2021, creating more than 400,000 jobs in the process.[2]

The App Association appreciates this opportunity to provide feedback to the CMA on its Strategic Market Status (SMS) investigations into Apple's and Google's mobile ecosystems.

App Association comments

Question 1 - Do you have any views on the scope of our investigations and descriptions of Apple's and Google's mobile ecosystem digital activities?

The relationship between large platform providers and small developers is symbiotic, and app makers use app marketplaces and platforms in three primary ways: to reach a global market, reduce complexity and overhead, and benefit from existing consumer trust. SMEs make business decisions about which platforms to make their products and services available on. That decision includes considering where their customers are, what tools are available, and the reliability of the underlying infrastructure. SMEs are able to take advantage of constantly improving tools and technologies as online marketplaces compete for their business.

[1] Tech UK - UK Tech SMEs: A Global Force to Be Reckoned With - 2023
[2] Deloitte – The App Economy in Europe – 2022

In return, mobile phones are made great by the software (apps) developed by small and medium-sized companies. SMEs are constantly finding new ways to solve problems and create opportunities built on top of the interwoven layer of tools and infrastructure many larger companies offer. In addition, digital platforms such as Apple's App Store and the Google Play store play a crucial role in fostering consumer trust by offering consumer protections, including secure payment systems, data privacy guarantees, and vetting processes for products and services. This creates an environment where users feel comfortable exploring new services and apps. These built-in protections benefit all developers but are especially valuable for SMEs, which often lack the brand recognition and established reputation of larger companies. Digital platforms help them access consumers to gain and maintain trust consumers based on the curation policies of the platform itself, making it easier for small companies to grow.

As paragraph 24 highlights, this ecosystem approach benefits consumers, who report high levels of satisfaction. However, the role of platforms in ensuring security and privacy should be more explicitly acknowledged. Paragraph 25 gives little space to this, even though security is likely a key reason why consumer trust remains high. Paragraph 26 also implies that deciding which apps are allowed on app stores is somehow separate from the security role of gatekeepers, when in fact, maintaining quality and safety standards is one of the most critical functions of these platforms. Similarly, paragraph 19 discusses app store standards without mentioning security or quality control as reasons for these standards. These omissions oversimplify the trade-offs involved in app store governance.

The App Association is also concerned about the figures presented on the size of the UK app economy in paragraph 17. In 2021, the App Association worked with Deloitte to measure the UK app economy, finding that direct revenues amounted to €38.4 billion, with advertising revenue accounting for €13.8 billion, paid downloads and in-app purchases generating €2.1 billion, contract work contributing €21.3 billion, and mobile commerce bringing in €1.2 billion. Indirect contributions brought the total impact to €86.5 billion, representing 1.5 per cent of the UK's GDP. The sector supported an estimated 400,000 jobs in the UK. Given this, it is difficult to accept that the UK app economy has shrunk since 2021, and it would be helpful to clarify how the CMA arrived at its estimates.

The CMA's discussion of in-app browsing should also be expanded and made more precise. It would be useful to clarify how the CMA defines in-app browsing, especially given that it plays an increasingly important role in digital interactions. In paragraph 23, artificial intelligence (AI) integration into operating systems is raised for the first time. This is a critical issue, as AI-driven operating systems could present security risks, particularly if they introduce vulnerabilities or reduce the ability of developers to maintain control over their own services.

The CMA's framing of platform control over app distribution does not capture the entirety of the market. While Apple and Google exert significant influence, they are not the only players shaping the market. For example, Samsung, a market leader in handsets, currently ships with multiple app stores, and Epic Games recently partnered with Movistar to preload phones with its own app store, demonstrating that alternative distribution models can and do emerge. These examples, relevant to paragraph 15, suggests that control over app distribution is more dynamic than sometimes presented. Similarly, paragraph 27 describes app store decisions as 'make or break' for businesses, but it does not include recognition that these processes prevent harmful apps from reaching consumers.

The investigation also groups together a range of issues that may not all be comparable in terms of risk and complexity. For example, paragraph 28 suggests that 'Super Apps' are more viable in other markets, such as India, but does not fully explore why this is the case. It is unclear why CMA

is attempting to make 'Super Apps' with multiple distinct features distinct from other apps in the context of its investigation. So called 'Super Apps' can have trade-offs in the area of privacy and security and aren't automatically better than other platforms.

Finally, in paragraph 37, there is an opportunity to consider the wider economic impact of regulatory interventions. The EU's ill-advised regulatory intervention into the curation practices of digital platforms that have enabled significant SME growth and job creation is only beginning to be implemented, with notable unintended consequences already becoming apparent. The CMA should recognise that the EU's approach to digital platforms has not yet demonstrated clear economic benefits and, given the CMA's objectives under its new leadership, it would be valuable to assess whether overregulation could harm the UK's competitiveness. To be blunt, the EU's aggressive regulatory stance has not been shown to enhance opportunities for SMEs or the EU's economic competitiveness writ large. In fact, the UK, with a history of lighter regulatory action, has outstripped the EU in small business success relative to population. The UK has an opportunity to take a more balanced approach that encourages competition while also enhancing security, consumer trust, and economic growth.

Question 2: Do you have any submissions or evidence related to the avenues of investigation set out in paragraph 70-72? Are there other issues we should take into account, and if so why?

It is critical for the CMA to understand that the vast majority of our members, and in fact the majority of all developers, build products for cross-platform use. In fact, for productivity apps, developers regularly build products for HTML5 web functionality and then enhance them for use with specific platforms or devices. The idea of building products that have low friction for consumers is assumed. However, a regulatory scheme that forces some kind of technical switching requirement could backfire terribly, and lead to less innovation of tools and microprocessors, with hardware companies simply building products that serve a lowest common denominator. Therefore, any regulatory mandates forcing platforms to scale back their curation practices intended to protect consumers through cybersecurity threat mitigation, privacy protection, and intellectual property enforcement will undermine the very commercial and technical viability of the digital economy. Mobile operating systems are designed with integrated protections that prevent malicious access and maintain performance, and these protections should not be undermined in the pursuit of competition.

Paragraph 70 is central to the investigation, as it sets out the precise criteria for Strategic Market Status (SMS). It is essential that these tests assess market power in a way that reflects not just competition concerns but also the broader implications for user experience, security, and technological advancements. The determination of SMS should not overlook the complexity of balancing innovation with consumer protection, particularly in markets where security, privacy, and device performance are critical.

Paragraph 71b makes an interesting reference to the internet of things (IoT). The broader issue is how mobile ecosystems extend across multiple devices and whether these integrations create competitive barriers or deliver legitimate consumer benefits. Companies like Meta have taken a different approach by offloading processing to cloud-based infrastructure rather than tying functionality directly to a smartphone OS. This raises the question of whether restricting ecosystem control would encourage alternative architectures or simply shift control to different gatekeepers. We encourage CMA to ensure that its efforts to not distort competition to prevent or otherwise disincentivise processing on device at the network edge, which is critical to reducing energy consumption by data centres.

The mention of AI integration in paragraph 71b highlights another critical concern. While the concept of AI is not new, the implementation models of AI are changing almost daily. AI-driven features require deep system access, which raises security, privacy, and intellectual property implications. Any regulatory mandates forcing OS providers to open access to third-party AI assistants would need to account for how these integrations handle sensitive user data, how they affect device security, how vital IP is protected, and whether they could reinforce market dominance for large firms already leading in AI development. Without an established AI regulatory framework, it remains unclear how AI-driven services should be governed in mobile ecosystems. Overly broad interoperability requirements could create risks that regulators are not yet fully equipped to address. At a minimum, CMA should clarify that its actions stemming from this investigation, targeted at "AI integration" or otherwise, will not compromise security, privacy, or intellectual property rights.

Additionally, there are concerns regarding how interoperability mandates could impact connected devices and mobile ecosystem functionality. First, unrestricted background execution could allow larger firms to offload intensive computing tasks onto mobile devices, impacting system performance and battery life while making it harder for smaller developers to compete fairly. Second, requiring OS providers to share Wi-Fi connection data with third-party devices would introduce privacy risks and potential GDPR conflicts, as forcing platforms to store and distribute network credentials raises security concerns. Third, changes to wireless security protocols could facilitate piracy and weaken digital rights management protections, which would harm content creators and developers that rely on protected distribution channels.

A proportionate approach is necessary. While fostering competition is important, regulatory intervention should not introduce vulnerabilities that compromise security, privacy, intellectual property, or fair market dynamics, which may in turn make it harder for small businesses to compete. Any measures related to AI integration, connected devices, or mobile interoperability should carefully assess potential risks to ensure that regulatory efforts enhance innovation rather than creating new challenges for developers, consumers, and businesses.

Question 4: Which potential interventions should the CMA focus on in mobile ecosystems? Please identify any concerns relating to Apple's or Google's mobile ecosystems, together with evidence of the scale and/or likelihood of the harms to your business; or to consumers.

As the CMA knows, mobile platforms provide essential infrastructure that enables small developers to reach consumers. These tools help to ensure that competition, innovation, and consumer trust remain at the heart of the UK's digital economy. There are areas where improvements could be made to create a more dynamic environment for businesses of all sizes.

One key area of concern is data portability. Ensuring users can control access to and transfer of their data—without compromising privacy and security—should be a priority. Technical protection mechanisms including encryption that enable a consumer to control access to the data apart from the platform are an important feature. Any intervention into mobile ecosystems must not inadvertently weaken security protections that underpin consumer trust in app stores and mobile platforms.

Any intervention must also be measured and proportionate. The vast majority of apps are built by SMEs, and while they often seek more flexibility and opportunities within mobile ecosystems, they do not want the fundamental infrastructure that enables them to operate effectively to be weakened. Developers may push for more favourable terms from platforms, but they do not want regulatory interventions that compromise security, reliability, or consumer trust.

App stores, payment processing, security measures, and platform-level consumer protections are integral to the success of small developers. Any interventions should focus on fostering a competitive environment where innovation can thrive while preserving the stability and trust that make mobile ecosystems work. The CMA should ensure that any changes imposed on digital platforms promote competition and choice without introducing unintended consequences that could harm the very businesses they aim to support.

Question 5: Are the potential interventions set out above likely to be effective, proportionate and/or have benefits for businesses and consumers?

SMS investigations target large technology firms but inevitably relate to and will impact the small businesses that leverage digital platforms to compete, grow, and create jobs. Some proposals, such as mandated sideloading and alternative app stores, weaken security, reduce consumer trust, and strengthen already dominant players.

For small developers, existing app marketplaces provide essential visibility, security, and distribution. Existing curation practices have helped create a thriving app economy. The assumption that scaling them back would broadly benefit SMEs ignores the risk that alternative stores will likely lack the same safeguards and consumer trust. Requiring Apple and Google to share their app catalogues, as suggested in paragraph 85(iii), is especially problematic. This strips developers of control over where their apps appear. Allowing alternative stores to piggyback off Apple and Google's app review processes while simultaneously criticising their role in app curation is contradictory and disincentivises alternative app stores from having their own strict security requirements. Without their own strict security controls, these stores could weaken the overall ecosystem.

Paragraph 85(iv) proposes allowing users to download apps directly from email links, raising serious security concerns. Malware distribution through deceptive emails is already a major cybersecurity risk. Lowering protections would increase threats to consumers and businesses. Google's existing sideloading warnings serve a purpose, and any modifications should prioritise user security over ease of sideloading. Being able to download apps from email links is especially worrying when considered alongside some of the CMAs other proposals that would allow these apps much greater access and control over consumers' devices and data.

Concerns over app store fees, as raised in paragraph 85(c), require more nuance. The claim that 'many' developers oppose the 30 per cent commission overlooks that almost no developers pay that rate. For 2023, nearly 97 per cent of Google Play and 96 per cent of Apple App Store apps are available for free. And it is estimated that less than 50 per cent of non-game apps use in-app purchasing, with an AppsFlyer study estimating that only 5.2 per cent of users spend any money on in-app purchases.[3] Furthermore, only apps that make more than $1 million pay 30 per cent, the rest are at 15 per cent or even less.[4] For them, platform services—including security, payments, and distribution—provide reasonable value.

Paragraph 85(c)(i) refers to FRAND (fair, reasonable, and non-discriminatory) platform access, but access should not be indiscriminate. Strict security and quality standards must prevent harmful, fraudulent, or insecure apps from gaining entry. The ability to remove or restrict unsafe apps is essential, and regulatory changes must not weaken this safeguard.

[3] AppsFlyer - New report on global in-app spending habits finds that Asian consumers spend 40% more in apps than the rest of the world - 2016
[4] Adapty - How much does an app make: Adapty's ultimate app revenue & VAT guide - 2024

On behalf of our members, the App Association urges policymakers to consider the impact of regulatory changes on SMEs and to consult carefully with small developers as part of any SMS investigation process. Any interventions should promote fair competition and innovation without creating new risks or eroding consumer trust. The UK's tech sector thrives on small businesses, and regulation should support their growth, not strengthen already dominant firms.

Q6: What key lessons should the CMA draw from interventions being considered, imposed and/or implemented in relation to mobile ecosystems in other jurisdictions?

The UK must carefully consider the impact of regulatory interventions in mobile ecosystems worldwide, particularly in the European Union, to avoid unintended consequences that could stifle innovation and harm SMEs. It has long been established that Europe's increasingly complex regulatory landscape has created significant burdens on small businesses, making it harder for them to compete and grow. The Draghi Report , representing a notable recent acknowledgement of this systemic flaw in the European Union's approach, highlights how Europe has clearly fallen, and continues to fall, behind due to over-regulation. Concretely, despite claims to encourage innovation, the Digital Markets Act (DMA) in Europe has introduced regulatory restrictions that disproportionately affect SMEs.

Nearly a year into the DMA, SMEs have yet to see the claimed benefits EU policymakers guaranteed in the leadup to its enactment. Instead, major issues are already emerging from the DMA's implementation, and there is more uncertainty than ever as to whether the DMA is fostering competition. For example, changes introduced by the DMA, such as the requirements for side-loading and offering unlimited alternative app marketplaces, benefit larger companies with established network effects but have little utility for micro-sized businesses and startups. This concern is also reflected in Atomico's 2024 *State of European Tech* report, which surveyed c.3,500 tech founders and investors. The findings show that **41 per cent are dissatisfied with the DMA**, **38 per cent see no significant change**, and only **22 per cent view it positively**. This data underscores that the regulation is failing to deliver meaningful benefits for SME developers, reinforcing the need for a more measured and effective approach.

The fact that the DMA's implementation is going beyond its original parameters and causing unanticipated disruptions is another serious worry. The introduction of new technology and services, including those based on cutting-edge artificial intelligence, has been delayed because of the DMA's compliance requirements for gatekeepers. This results in a fragmented and less lucrative market for developers, which eventually stifles innovation and growth in the app industry. The UK, on the other hand, is well positioned to observe the impacts of a regulatory intervention aimed at solving undemonstrated and hypothetical problems so that the mistakes made in both policy and implementation by the EU are not repeated. With the SMS determination, the UK must prevent a similar result. Regulators must continue to pay attention to concerns about consumer trust, privacy, and security.

Conclusion

The App Association welcomes the opportunity to contribute to the CMA's SMS investigations. SMEs drive the UK's digital economy, and the UK has a chance to take a balanced approach, avoiding the harmful unintended consequences seen in other jurisdictions, where overregulation has burdened SMEs while reinforcing the dominance of large firms. Policymakers must ensure interventions enhance competition without disrupting the stability of digital ecosystems.

We look forward to working with the CMA to support a fair, secure, and innovative app economy.

Sincerely,

Mike Sax
Founder and Chairperson

Stephen Tulip
UK Country Manager