DMA trilogue - Comments on 6.1.f

Apple opened the iOS platform to third party development in 2008. It created a set of software tools, a set of standard application programming interfaces (APIs) to iOS for developers, and a distribution platform, the App Store. Apple offers developers an extensive set of software tools, frameworks and services. The original software developer kit had fewer than 10,000 APIs. Today, we make more than 150,000 APIs available to developers for iOS alone. Apple's decision to open iOS in 2008 created a completely new and unique technology environment that has resulted in an explosion in software development, thereby fostering competition and innovation.

The access provisions under Article 6.1.f have been justified as being necessary to ensure that business users have access to the same same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services. In order to deliver a workable and effective DMA, access obligations must be proportionate and defined narrowly while allowing continued innovation and ensuring predictability and legal certainty for all actors. Access obligations must not endanger user safety, create cybersecurity threats, harm data privacy, or otherwise impair the integrity of the platform.

The introduction of relevant safeguards to ensure end-user security and data protection are very much welcomed. However, an unfettered expansion to the scope of the 6.1.f, without any nexus to ancillary services, a broad definition of "interoperability" and prescribed conditions of access would undermine both legal certainty and seriously impact the ability to innovate both as regards the functionalities of operating systems and how they can be accessed by third parties.

In support of end-user security and data protection safeguards

As evidenced by this latest Eurobarometer report, EU citizens very much care about cybersecurity and the protection of their data. 56% of EU citizens polled said they were worried about cyber-attacks and cybercrime (e.g. theft or abuse of personal data, ransomware, phishing). 46% were concerned about the use of personal data and information and information by companies or public administrations.

In this light, it is crucial that the DMA does not inadvertently limit the ability of engineers within gatekeepers to tackle ever-evolving cyber security threats and continue to innovate in the field of data protection and data minimisation. We **therefore call on the negotiators to support the introduction of safeguards, as proposed by the European Parliament, allowing gatekeepers to take measures to ensure that functionality access does not endanger end-user data protection or cyber-security**. The negotiations should also consider **including a reference to user safety**.

This would allow Apple to:

- Take action should we have evidence of specific third party software that leverages functionalities in a way that poses cyber-security threats, without necessarily seeking to attack the integrity of the hardware, software and OS. Today, we are able to do so by suspending a risky app on the App Store, leveraging the developer program to work with the developer and fix problematic practices, and using malware removal capabilities to quarantine or delete the offending app. For examples, please look at Apple's Side-loading White Paper, which includes amongst others a case study of Goontact (p. 21). This spyware seeks to abuse the privileges of the Apple Developer Enterprise Programme to trick users into downloading spyware and giving access to personal data for blackmail purpose (p 21).
- Continue innovating in the field of OS, hardware and software data protection, notably linked to data minimisation. Over the last decade, Apple has, in response to public concern about illicit uses of location data, updated the controls available to users in order to 1) provide them with real control over how their location may be tracked and for what purpose, notably by allowing location to be available only while a user is using an app, and by enforcing that option when some developers sought to not offer it, offering a "use it once" option; 2) enhance transparency so that users who grant always-available location-sharing receive a reminder with a visual representation of where they have shared data to help inform their

choice; and 3) give options for developers to only receive coarse location data while 4) still offering tools to help third party developers innovate on the basis of location data (relevant mapping information, location-relevant recommendations, etc). We have shown that innovation in this area can take place in a way that need not undermine privacy and security, and the DMA should not prevent us from continue to do so in the future.

- Continue to limit the ability of business users to abuse device functionalities in ways that would impact the safety of individual users, beyond applicable product safety legislation. This could include, for example, the ability to tamper with audio levels, or to use devices and operating systems to track users without their consent or knowledge.

Scope of 6.1.f

The extension of the scope of 6.1.f, as proposed by the European Parliament, raises important concerns.

Firstly the European Parliament proposes the introduction of an unfettered right to access operating system, hardware, and software features and functionality to any 'services' or 'hardware' providers, regardless of whether they are a business or user of the platform. This risks turning 6.1.f into a Pandora's box of unintended consequences, where any OS, hardware or software functionalities or related services could be targeted, regardless of whether they impact market contestability.

Under this expanded scope, third parties could claim access to a virtually limitless set of functionalities, including but not limited to:

- secure chips and biometric recognition technology, sensors like microphone, camera, location, and many others that are linked to fitness and health - all while bypassing system protections and user choices;
- detailed device characteristics, like raw sensor data, that would allow third party apps or services to bypass privacy protections, enabling detailed tracking of users;
- the ability to manage background processing or battery performance/safety;
- the ability to bypass audio level restrictions that protect users from hearing damage;
- underlying functionalities which power our accessibility features - a third party app or service with such access could read a user's email, obtain every keystroke a user made (personal ID numbers, credit card numbers), see every website the user goes to, including encrypted ones such as banking websites, and even possibly initiate actions on the user's behalf. This would result in a complete bypass of system security and privacy protections;
- the ability to modify telephony/baseband software which could allow modified devices to negatively impact cellular networks.

Given that operating systems is described as a service in the DMA (i.e. a core platform service) this could allow alternative OS providers to request that iOS be replaceable altogether on iPhones. This would fundamentally reduce competition in devices markets, making impossible for Apple to offer an integrated, curated alternative to licensed operating systems.

Secondly, the European Parliament extended the scope of functionalities to be provided to third parties competing with the gatekeeper's ancillary services to include software features "*regardless of whether these software features are part of an operating system*". This could be interpreted broadly as mandating access by third party competitors to functionalities and technologies that are not part of a core platform service, potentially including server-based software processing, data center access, algorithms, disaster recovery centers, etc. Even if focused on contestability in ancillary services markets, this goes far beyond the aim of the DMA to limit uncompetitive or unfair leveraging of a core platform. It would also raise new security concerns, giving malicious players avenues to attack the core infrastructure of the core platform service placing the entire core platform service at significant security risk.

Each of these scope extensions raises fundamental concerns over the ability of a company, regardless of its size, to benefit from legal certainty, to innovate for the benefit of all users, and to

protect its intellectual property. This would be the case even with the inclusion of safeguards highlighted above, as it would put the burden on the gatekeeper to justify such safeguards following third-party claims of access.

In this light, **we call on the negotiators to confirm the scope of 6.1.f as proposed by the European Commission** and to specify in the recitals that 6.1.f should focus on functionalities that are key to deliver market contestability, based on clear evidence.

Definition of interoperability

The European Parliament has proposed a new and overly broad definition of interoperability (Article 2.1.23b) that could have serious impact on innovation and be virtually impossible to implement in practice.

Firstly, the reference to a "*mutual exchange of information* across *all hardware and software elements"* could be interpreted as imposing full service interoperability across all relevant obligations of the DMA, including 6.1.f. This would be vastly disproportionate, going far beyond the intention of the draft DMA to ensure relevant functionalities are accessible to relevant third parties. This would also be practically impossible without the development of (yet to be defined) common industry standards to cater for such mutual exchange of information. We have already seen the need to rely upon such standards with the implementation of data portability within the GDPR.

Secondly, the last sentence, which seems to dismiss access *using "an application software or other technologies for conversion",* could be interpreted as precluding functionality access through APIs, or application programming interfaces - despite this being standard industry practice and by far the most efficient and stable means to achieve interoperability.

Coupled with the practice of app "sandboxing" (in essence, a unique home directory for an app's files on the OS), APIs are the most appropriate way to enable and deliver OS functionality access to developers, including new or enhanced OS functionality as it develops over time, while ensuring that third party apps leveraging such functionality continue to work (these apps don't "break" when the underlying functionality changes or evolves) and such access does not undermine the integrity, security and data protection of the operating system or of other third party apps.

In this light, **we call on the negotiators to talk on board the language proposed by the European Commission and the Council General Approach**. Given the breadth of established industry practices to ensure interoperability and/or software and hardware access, this should not be explicitly defined in the DMA.

Conditions of access

Both the European Parliament and Council introduced language to frame conditions of access to OS functionalities covered by 6.1.f. Each were added without thorough assessment of impact on the market.

The European Parliament text would mandate that all access to OS, hardware and software functionalities should be "*free of charge*". This would equate to a full expropriation of valuable intellectual property and, at that scale, seriously undermines a gatekeeper's freedom to do business in the EU single market (in breach of EU law).

The Council of the EU proposed that OS functionalities falling in the scope of 6.1.f should be accessed on conditions that are "*fair, reasonable and non-discriminatory*". Given the difficulties of assessing FRAND obligations in practice, this would lead to significant legal uncertainty, paving the way for both a litigation-driven definition of this article and a very heavy enforcement burden for the regulator.

Mandating conditions of access requires case-by-case economic, legal and technological analysis, and cannot not be tackled in catch-all manner. We thereby **call on the negotiators to revert back to the language proposed by the European Commission**.