Kluwer Competition Law Blog

Apple's DMA Compliance Workshop – The Power of No: Breaking Apart the Bundle?

Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Tuesday, March 19th, 2024

The Digital Markets Act (DMA) became entirely applicable on 7 March 2024. By then, the gatekeepers issued their compliance reports documenting their technical solutions and implementation of the DMA's provisions under Article 11 DMA as well as their reports on consumer profiling techniques as required under Article 15 DMA (see here).

During the following week, I will be covering the workshops organised by the European Commission per each of the gatekeepers under *The Power of No* series, where the representatives of the undertakings meet with stakeholders to grind their compliance strategies and solutions. This blog post covers the first workshop held by the EC for assessing Apple's compliance solutions.

Apple's compliance strategy: short, digestible and moving-target-like!

Apple has been preparing for some time now to face a major backlash against its proposed implementation of the DMA. In January, it first outlined via a press release and dedicated documentation its solutions to address the DMA's desire to open up markets to pursue the goals of contestability and fairness (see comment on that first set of proposals here).

At that time, the gatekeeper formulated one of its major concessions to the DMA: it would allow for the alternative distribution of apps at the upstream level (by allowing alternative marketplace apps to set up their own app stores on iOS) and at the downstream level (by allowing developers to distribute apps on iOS but not on the App Store). In parallel, Apple also proposed to introduce an alternative set of terms that third-party developers could opt in into, which establishes a re-furbished version of Apple's existing fee model. For instance, the generally applicable 30% fee imposed on digital services and products would be automatically reduced to 17% for major developers, whereas it also introduced a wide array of different fees to cover the value delivered by the ecosystem to developers.

The proposal did encompass huge criticism on the side of developers, and Apple encountered three main trainwrecks leading towards the compliance deadline (and after it!). First of all, Apple announced that as a result of enabling alternative distribution on its ecosystem, it would have to stop catering to the possibility of offering progressive web apps on iOS. That is, Apple's functionality to include sites on an iPhone's home screen. Second, on the 6th of March, Epic Games voiced concern about Apple's (unjustified) suspension of its newly created developer account. Apple backtracked its initial decisions on both counts. It now continues to offer progressive web apps on iOS and reinstated Epic's developer account following regulatory pressure. Additionally, on the 14th of March, Spotify also denounced that Apple is stalling its app updates to hinder its new functionality from being rolled out as a consequence of the DMA's implementation.

If anything, Apple's implementation of the DMA is fragmented into different sets of documentation. On one side, it issued a 12-page long compliance report on 7 March 2024 accounting for the solutions that it has implemented (and is expected to develop and roll out in the coming months) in response to the regulatory framework's high expectations. On the other hand, during the last few days, it has repeatedly updated, through press releases and by issuing additional developer documentation, its technical implementation of the regulation.

Against this background, Apple's representatives presented their compliance solutions around the DMA before stakeholders and the European Commission which revolved around four main workstreams, including the gatekeeper's implementation of: i) its choice screens and default settings relating to Safari, iOS and the App Store under Article 6(3) DMA; ii) its all-encompassing transformation of app distribution under Articles 5(4), 6(4) and 6(12) DMA; iii) its solutions on effective interoperability and anti-tying under Articles 5(7) and 6(7) DMA; and iv) its data-related obligations under Articles 5(2), 6(9) and 6(10) of the DMA. The post considers each one of them in turn, remarking on the main points of contention discussed in the workshop.

The default browser is out of the window, but how will it work?

Apple reiterated its approach to applying Article 6(3) of the DMA – to ensure that end users are presented with a choice screen so that they can choose any type of web browser to be their default across the iOS ecosystem. Since Apple's most recent update on iOS 17.4 was rolled out on iPhones, upon the user's first use of Safari, Apple presents a prompt with 12 different choices of different browsers to select as one's default browser. The user is forced to scroll down through the prompt to select the preferred browser which will, then, become its default, albeit that the selection does not automatically trigger the download of that alternative browser if that were to be different from Safari. Those alternative browsers are displayed based on their prominence across each of the Member States so that the same list will not be streamlined in the EU.

The stakeholders pointed out, however, that the choice screen's effectiveness may be undermined by its short-lived impact. It will only apply once the user first uses Safari. That is to say, the prompt will not be shown, for example, once every year to ensure contestability, despite that the list of providers may change over time. Furthermore, the choice screen is only displayed on Apple's proprietary web browser. In other words, when users access other alternative browsers, the choice will not be displayed. Let's say that the user only uses Chrome on the iPhone. In that case, the choice screen will not be displayed at all for that particular user.

According to Apple, that list is elaborated in line with objective and consistent methodology drawing from third-party sources. Asked by the participants of the workshop, Apple recognised that the criteria that it chose to list the alternative browsers derived first and foremost from the most downloaded browsers on the App Store, as well as from third-party data resources that the EC had pointed out through the iterative process of tailoring its compliance solution towards the deadline. On top of that, the browser apps that can qualify to appear on that 12-item list must neatly fall within the category of browser apps and they must have been downloaded, at least, by 5,000 users on EU App Store storefronts in the prior calendar year. This is the reason behind the fact that Apple has created the Default Browser Entitlement so that browser apps may access the list when meeting the specific functional criteria set out by the gatekeeper.

In general, Apple acknowledged that the choice screen is delivering its first results, insofar as alternative browsers such as Brave, Mozilla and Vivaldi have seen a surge in the number of people installing their web browsers. The immediate results may, however, have been overstated insofar as stakeholders repeatedly remarked on the fact that alternative browsers had no cognisable way of learning if those downloads followed the user's installation of their apps as a consequence of Apple's choice screen. In fact, the gatekeeper does not provide any information directly to these alternative web browsers.

New app distribution, fee model and anti-steering provisions

Article 6(4) DMA compels gatekeepers to enable their operating systems for the installation and effective use of competing app stores and sideloading from web apps, whereas Article 6(12) provides that gatekeepers must provide access to their app stores on FRAND terms. As pointed out earlier, Apple has entirely opened alternative app distribution on its ecosystem. Thus, users will have up to three types of ways in which to download apps on their iPhone devices: i) through an alternative app marketplace, which may distribute only proprietary apps or apps of third-party developers; ii) directly via the web (sideloading); and iii) via the proprietary App Store.

The old man and the fee

To implement those changes, Apple has designed two different types of business models that developers may rely on when distributing their apps on iPhones. On one side, they can remain as they already are, by distributing apps exclusively via the App Store, and the traditional terms and conditions will apply to them. In monetary terms, that entails that all digital services and products will be charged with the 30% fee (or the 15% fee if the particular developer belongs to the App Store Small Business Program).

On the other side, developers that want to distribute apps on other storefronts different to the App Store, are forced to opt into the Alternative Terms Addendum for Apps in the EU. Those terms imply to the developers that a completely distinct fee structure and model will apply to its operations. The 'general' fee structure is reduced from 30% to 17% on digital products and services (and reduced to 10% for those belonging to the Small Business Program). On the contrary to its previous press release, Apple recognised at the workshop that the general fee will only apply to those digital goods and services that are distributed on the App Store. Additionally, those developers that distribute on alternative marketplace apps will be bound by the Core Technology Fee (CTF), which will charge developers EUR 0,50 per first annual install. 'Regular' developers are held distinctly to the developers of alternative marketplaces: the former are exempted from paying CTF up to one million downloads, whereas the latter apply the CTF to each first annual install. Finally, developers may be charged an additional 3% if they decide to continue using

Apple’s proprietary in-app purchase (IAP) functionality.

In Apple’s own words, the dual system of the two sets of terms is explained due to a fundamental reason. Since it was first introduced, Apple has operated and charged developers for the value they created for them in a bundle. That is to say, Apple catered to a myriad of services, technology and tools provided to the developers, and they were all factored into a single 30% commission. However, since alternative distribution has been forced upon the gatekeeper, then it has been forced to allocate a price for each one of them. For instance, the CTF accounts for all of the technology, tools and services that Apple makes available for developer to support them when launching their apps, such as their 250,000 APIs and machine-learning approach. Similarly, the reduced 17% fee now reflects the value that they deliver in app discovery and distribution on the App Store. Due to this reason, Apple will not charge that fee to developers who do not distribute apps on their proprietary software application store.

Moreover, Apple also expanded on the fact that it wanted to provide adequate choices for developers to select whether they wanted to remain within the existing terms or whether they preferred to shift to the new fee structure and model. Even if that were true, however, Apple recognised that it would provide for the one-off possibility that developers who have opted into the new terms may switch back to the traditional and customary arrangement. In Apple’s own words, these terms -both the old and the new- are FRAND in the sense of Article 6(12) insofar as they transversally apply to all types of developers, despite of their size or type.

Alternative distribution: it’s not all new and shiny

Despite the apparently satisfactory move towards allowing alternative distribution on iOS, Apple went into great detail to establish that alternative marketplace providers and the alternative distribution of apps come with great risk to their device’s security, safety and privacy, as they already did in a recent White Paper published a few weeks back. This is precisely the reason why alternative distribution adds fundamental steps to the way in which Apple controls its ecosystem. Instead of reviewing apps directly through the App Store, when marketplace providers and developers wish to distribute on alternative storefronts, they will be held accountable to comply with a list of requirements to be available on iOS.

They will face Notarisation, which basically entails that Apple will green-light every single marketplace provider and developer so that it can develop its alternative (and competing) software application store or app. Notarisation is a baseline review applicable to all alternatively distributed apps focused on platform policies which combines automated checks and human review. Stakeholders raised concerns about the fact that Notarisation already applies to Apple’s Mac for web distribution of apps and the two processes are fundamentally different one from another. As opposed to Mac, Notarisation on iOS is much more demanding. According to Apple, one’s smartphone stores one’s most sensitive data so this element justifies that Notarisation requirements are enhanced for iOS. Furthermore, Apple expects that alternative marketplace developers will issue their own guidelines to moderate content as well as to inform users about their business practices in their own software application stores.

On the side of sideloading (that is, downloading apps directly from the web), requirements upon developers are not left adrift, either. To make apps available directly on the Internet and for them to be downloadable on iOS, Apple requires that developers must be enrolled in the Apple Developer Program as an organisation (or at the user level) in the EU for two continuous years or more and have an app that had more than one million first annual installs on iOS in the EU in the prior calendar year. In other words, developers that want to cater to their apps exclusively via the web will not be able to do so if they do not have a previous record with Apple, be that through alternative distribution or the App Store.

Interoperability and web browser engines un-tying: it all comes apart

Article 6(7) requires that gatekeepers provide free of charge interoperability to their hardware and software features accessed via the operating system, whereas Article 5(7) DMA prohibits the gatekeeper from requiring end users or business users to interoperate with an identification service, a web browser engine or a payment service in the context of the services provided by the business using that gatekeeper's CPS.

Interoperability, lacking any context

Apple has established a dedicated process for DMA interoperability with iOS and iPhones where developers may make submissions to Apple so that the gatekeeper decides whether it can cater to those interoperability solutions individually. In principle, Apple adopts this 'black box' approach because it cannot simply offer access to an API without compromising security, it argued throughout the workshop. For instance, if an individual application manages the control of the allocation of the device's processing, then the device may not produce an urgent push notification or provide for basic functionality such as phone calls. This is the reason behind the fact that the solution to comply with the mandate of interoperability is also designed around the presence of entitlements placing the necessary guardrails to hinder bad actors from accessing sensitive information.

In Apple's response to stakeholders' questions relating to its black box approach, the gatekeeper recognised that it did have to perform the evaluation of these requests individually and perform intensive scrutiny internally so as to understand the interoperability request and figure it whether it could implement it in the short time. Significant engineering resources, attention and time from Apple are required to attend to the interoperability requests, although Apple's proposed solution is quite different to the implementation of other gatekeepers which have provided extensive interoperability solutions for particular types of services, and have not tried to obscure the process in the interim.

Alternative browser engines: WebKit, no more

Prior to the DMA's implementation, alternative web browsers could only operate if they were developed on the basis of Apple's proprietary WebKit, which required extensive efforts by competitors to adjust their services to the gatekeeper's ecosystem. Article 5(7) DMA forced Apple to un-tie the hands of competing browsers so that they could develop their apps on distinct browser engines as opposed to WebKit. Therefore, from now on, browser apps may include browsing experience on other browser engines other than WebKit.

Once again, Apple’s strategy in opening up its ecosystem is nothing short of imposing additional requirements upon developers. Browser apps must be authorised via BrowserEngineKit and BrowserEngineCore to incorporate those changes into their apps.

To qualify for the entitlement, the browser app must, then, present a separate binary from any app that uses the system-provided web browser engine. This is one of the most salient decisions that browser apps developers will have to make, as elucidated by one of the participants in the workshop. If browser apps have to submit a new binary to incorporate alternative browser engines into their services (that is to say, they have to be re-submitted for review via the App Store), then a clear consequence is expected to be produced with relation to the effectiveness of the choice screen solution contained under Article 6(3). The choice screen displays 12 of the most popular browser apps that must count with at least 5,000 downloads on EU storefronts on the App Store. Thus, by submitting a new binary, then the browser’s popularity may well vanish into thin air concerning its particular impact on compliance with Article 6(3). Against this background, the effectiveness of the solutions proposed by Apple around Article 5(7) may directly undermine the beneficial effects that the choice screen of browser apps seeks to ensure. Apple did not deny that this unintended consequence could be produced as a consequence of the browser app’s choice to submit a new binary for incorporating an alternative browser engine.

Data-related obligations: no choice screens and in-scope data

Apple’s approach towards protecting personal data does not come short of being compelling. In short, the gatekeeper believes that it does not use process or cross-use personal data across its core platform services or that it does profile consumers in any substantial way.

As opposed to the rest of the gatekeepers that have interpreted the provision under Article 5(2) as an open gate to introduce additional consent screens upon the users to basically override the prohibition of processing, cross-using, and combining personal data across core platform services, Apple has chosen to not confront users with such an implementation. In fact, it has adopted the opposite implementation: where it identified cross-uses or combinations of personal data prohibited by the DMA, it ceased to use App Store data in the context of other services and vice versa. On the side of their use of business user data in the context of the prohibition under Article 6(2), Apple clearly called that it focuses on making sure that it identifies in-scope data across its services to mark it appropriately so that it is only used for the initial purposes that it was processed and collected for. In that particular sense, Apple confirmed that it also keeps its datasets apart from those of its developers when they are in competition within it not only at the EU level but on a worldwide basis.

On the side of its technical implementation around Article 6(10) relating to its provision of data to developers of their self-generated data across Apple’s services, the gatekeeper first established that they aimed to minimise the amount of data collected or shared by Apple and that they only did so at the App Store level, whilst they did not perform data collection on iOS or Safari. To that particular aim, Apple expanded on the solutions that it presented within its compliance report and established that it would cater to providing deep insights on dashboards and reports for developers so that they can measure their app’s performance on App Analytics both through APIs and web interfaces. Therefore, Apple highlighted that it would be expanding the available analytics for developers to deliver even more insights to them, albeit without having to identify end users at the user level.

The same robust approach towards data was not particularly evident, however, when Apple presented its solutions to comply with the portability obligation under Article 6(9) DMA. The undertaking basically went over the promises that it had first established on its compliance report relating to portability which will only apply to a limited extent to: i) enable end users to export their personal App Store data to authorised third parties by them; ii) to help mobile operating system providers develop more user-friendly solutions to transfer data from iPhone to non-Apple phones (available in the fall of 2025); and iii) to enable browser switching solution for exporting and importing relevant browser data into another browser data on the same device.

Key takeaways

Instead of a stakeholder workshop, Apple's DMA compliance workshop was more of a monologue than an engaging and impactful dialogue with third parties. On their own merits, some of the solutions proposed by Apple may meet the threshold of not being blatantly contrary to the DMA's goals of contestability and fairness but there are still many tenets of the gatekeeper's technical implementation of the regulation that remain elusive and conflictful.

Although the all-encompassing solution of re-working its own fee modelling and structure may have caught (most of) the stakeholder's attention for the time being, effective compliance with the regulatory framework stands a long way ahead of the European Commission. Day 1 of the DMA's compliance workshops delivers on much ground yet to cover and a few impending questions on how a dual model of business terms, that obliviates compliance by default, may meet the high regulatory standard of the regulation.

This entry was posted on Tuesday, March 19th, 2024 at 8:30 am and is filed under App stores, Apple, Designation Decision, Digital, Digital competition, Digital economy, Digital markets, Digital Markets Act, European Commission
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.