CPI Columns
Europe

June 2024

Lessons for the DMCC: Challenges and Trade-offs Facing Access to Ecosystems in Digital Markets

By Nitika Bagaria and Arzu Mammadova | Keystone Strategy

Lessons for the DMCC: Challenges and Trade-offs Facing Access to Ecosystems in Digital Markets

By Nitika Bagaria[1] and Arzu Mammadova[2]

Disclosure: One of the authors has advised a third-party in various jurisdictions on some of the matters discussed in this article.

Introduction

The Digital Markets, Competition and Consumers Bill ("DMCC") finally came into effect in the UK on May 23, 2024.[3] Under this bill, the digital activities of certain firms can be designated as having Strategic Market Status ("SMS"). Designated firms will then need to meet certain obligations that will be set by the Competition and Markets Authority ("CMA") on a firm-by-firm basis. The CMA could also impose remedies through Pro-Competitive Interventions ("PCI"). The CMA has indicated[4] it expects to initiate 3-4 SMS investigations in the first year of the bill.

The experience from the Digital Markets Act ("DMA") that came into effect in May 2023 in the European Union ("EU") suggests that SMS firms are likely to defend their conduct on security and privacy grounds. This article discusses the trade-offs that the CMA will likely need to consider in its SMS designations – the trade-off between enforcing fair access to platform features on the one hand and protecting user privacy and security on the other.

The article then discusses these trade-offs in light of the recent DMA compliance announcement by Apple and related cases in the U.S. Finally, we discuss the implications for third parties who would benefit from platform access and companies challenging their SMS status.

We argue that, in its SMS investigations, the CMA will need to get into the nitty-gritty of the technology, much like the parties involved in recent litigations against Apple and Google in the U.S., to understand the extent to which conduct is justified by technical and security concerns and assess the viability of certain conduct requirements.

Platform Access in Digital Regulations

Under the DMCC, a firm designated an SMS is prevented from restricting interoperability between its relevant services or digital content and third-party offerings. Moreover, such firms are restricted from controlling users' engagement with the relevant digital activity.[5]

Ensuring fair and transparent access to platforms has been top of mind among competition regulators in various jurisdictions.[6] For example, in the EU, the DMA mandates gatekeepers to technically enable third-party apps and app stores on their operating system (Article 6(4)); prevents them from self-preferencing their services (Article 6(5)); and ensures they provide third parties with access to their operating system, hardware, and software features (Article 6(7)). Such requirements are aimed at promoting contestability and preventing platforms from obstructing competing firms' ability to offer equivalent services.

In a similar vein, in its recent lawsuit the DOJ alleges that Apple maintains a monopoly over smartphones by selectively imposing contractual

---

[1] Nitika Bagaria is a Senior Principal at Keystone Strategy. She holds a Ph.D. in Economics from LSE. Her previous professional experience includes roles at the UK competition regulator and in competition economics consulting.

[2] Arzu Mammadova is a Senior Software Engineer at Keystone Strategy. She holds a B.Sc. in Computer Science from Cornell University and brings professional expertise in assessing the technical aspects of legal and regulatory matters within the technology sector.

[3] UK Parliament, Digital Markets, Competition and Consumers Bill - Parliamentary Bills - UK Parliament, May 2024.

[4] CMA, "Overview of the CMA's provisional approach to implement the new Digital Markets competition regime (publishing.service.gov.uk)," January 2024.

[5] DMCC bill, see Article 20(3)(e) and (f).

[6] In addition to the EC, CMA and the FTC (US) discussed in the draft, the Japan Fair Trade Commission and South Korean Communications Commission are among many other regulators considering regulating access to mobile operating systems. See, for example, Nikkei Asia, "Japan to crack down on Apple and Google app store monopolies - Nikkei Asia," December 2023; and Mlex, "Apple, Google face hefty fines for app-store violations, South Korean watchdog says," October 2023.

restrictions on and withholding critical access points from developers.[7]

A common trade-off that competition authorities grapple with is between enforcing equal access to platform features on the one hand and protecting user privacy and security on the other. For instance, the CMA has been scrutinizing the restrictions imposed by Apple (and to a lesser extent Google) on a series of services, including third-party browsers, cloud gaming apps and alternative distribution channels, as part of its recent investigations into mobile ecosystems and the cloud gaming market.[8] While acknowledging the importance of Apple and Google opening up their ecosystems to competing products, the CMA is rightly aware of the importance of considering the impact on security when designing potential remedies.[9]

Similarly, the DOJ's lawsuit alleges that privacy and security concerns do not justify Apple's conduct.[10] Apple allegedly restricts alternative apps or services that are likely to be more secure and protect privacy. The Federal Trade Commission ("FTC") also recently acknowledged the trade-off between interoperability and security, but highlighted the importance for enforcers to closely scrutinize security or privacy-led defence of practices that restrict competition.[11]

As competition authorities increasingly recognize these trade-offs, they are integrating them into the regulations they enact. For example, the DMA provides that a gatekeeper is allowed to take "*strictly necessary and proportionate measures*" to ensure that interoperability does not compromise the integrity of its core platform service, such as the operating system or hardware or software features provided by the gatekeeper.[12]

So, how does an authority or a business evaluate whether access is a reasonable (technical) expectation and wouldn't compromise customer privacy or weaken security standards? Conversely, how does one determine whether the security measures in place (or proposed in response to pro-competitive interventions) are justified and do not unduly hinder access and innovation?

In the next section, we highlight this trade-off in the recent DMA compliance announcement by Apple and the related cases in the U.S.

Case Study: Apple's DMA Compliance and Related Lawsuits

Apple has historically imposed restrictions on alternative app distribution channels in its mobile operating system, iOS. The company has justified these restrictions on the grounds of security, claiming that enabling the installation of apps from alternative sources – often referred to as "sideloading" – either via a user directly downloading apps from a webpage or downloading an alternative app store, would compromise the security and privacy protections that make its devices safe.[13] Despite years of effectively resisting calls to open up its ecosystem, Apple is finally being made to comply in the EU following the European Commission's ("EC") designation of iOS, Safari, and Apple's App Store as "core platform services" under the DMA. On January 25, 2024, Apple announced the long-awaited changes to its policy for these products, which subsequently went into effect on March 7, 2024.[14] The EU has since opened a

[7] Department of Justice, "Office of Public Affairs | Justice Department Sues Apple for Monopolizing Smartphone Markets | United States Department of Justice," March 21, 2024.

[8] CMA, "Mobile browsers and cloud gaming market," January 2024.

[9] CMA, "Mobile ecosystems – market study final report," June 2022.

[10] Department of Justice, "Office of Public Affairs | Justice Department Sues Apple for Monopolizing Smartphone Markets | United States Department of Justice," March 21, 2024, paragraphs 141-147.

[11] FTC, "Interoperability, Privacy & Security," December 2023.

[12] See Article 6, paragraph 7.

[13] Apple, "Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading," October 2021.

[14] Apple, "Apple announces changes to iOS, Safari, and the App Store in the European Union," January 2024.

non-compliance investigation under the DMA into Apple's revised rules for app stores on iOS.[15]

Among the company's new offerings are developer tools and APIs[16] that enable the creation and installation of third-party app stores, which Apple refers to as "alternative app marketplaces," along with the installation of apps through these stores.[17] These offerings are accessible to developers with apps in the EU, who "consent" to Apple's new business terms.[18] Once developers agree to the new terms, they will have a one-time option to revert to the old terms, as long as they have not distributed an alternative app store, distributed apps *through* an alternative app store, or used alternative payment processing or linking out (i.e. redirecting users to the developer website to purchase digital goods or services). In other words, Apple only allows developers to switch back to the old terms if they have not yet taken advantage of any of the freedoms enabled by the DMA, essentially rendering the switch irreversible.

In parallel, Apple is introducing a series of controls to alleviate the "new risks the DMA poses to EU users."[19] These include enhanced on-device protections against malware that apply to all apps regardless of their distribution channel, authorization for prospective developers of third-party app stores, and a centralized notarization process for all third-party apps – a combination of automated and human-led checks, which scan apps for security threats prior to distribution. Notably, the new notarization process is an extension of notarization on macOS, Apple's operating system for desktops and laptops. Apple claims that macOS notarization has "worked well," which prompted its adoption on iOS.[20] This goes against Apple's persistent opposition to this very idea in the *Epic v. Apple* lawsuit, where it made claims that macOS had a "malware problem" compared to iOS[21] and that adding a necessary human review element to implement notarization on iOS would not scale well.[22] This raises real questions about the consistency and the reasoning behind security-based limitations Apple imposes.

Apple's security measures in response to the DMA may appear appropriate at first glance, given the expanded "attack surface" that inevitably results from introducing additional distribution channels. However, a look into the underlying details raises several questions about the proportionality of the required steps compared to the actual security risks involved. For instance, Apple continues to exercise a significant amount of control and apply technical hurdles on the alternative distribution of apps in its ecosystem in several ways. In particular, Apple imposes a variety of barriers on third-party app stores, requiring users to navigate extra steps to enable their use, such as:

To install a third-party app store, a user will need to first approve it by making the effort to navigate separately to the "Allow Marketplace from Developer" control in Settings, before going back to proceed to download it.[23]

Further, a user will be shown an additional screen summarizing the information about the third-party app store before completing the installation.

The user will encounter the same screen every time they attempt to install an app *through* the third-party app store as well.[24]

This additional friction is not warranted from a security perspective, given that every alternative

[15] EU, "Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act," March 2024.

[16] Apple, "Apple announces changes to iOS, Safari, and the App Store in the European Union," January 2024. Apple's announcement also includes enabling developers to use alternative browser engines and alternative payment processing for in-app purchases.

[17] Apple, "MarketplaceKit: Create an alternative app marketplace or distribute your app on one."

[18] Apple, "Alternative Terms Addendum for Apps in the EU."

[19] Apple, "Apple announces changes to iOS, Safari, and the App Store in the European Union," January 2024.

[20] Apple, "Complying with the Digital Markets Act: Apple's Efforts to Protect User Security and Privacy in the European Union," p.6., March 2024.

[21] See United States District Court, "Rule 52 Order After Trial on the Merits," p. 113., September 2021.

[22] See United States District Court, "Rule 52 Order After Trial on the Merits," p. 148., September 2021.

[23] Apple, "Alternative distribution user experience."

[24] This will be the case unless a user makes the third-party app store their default marketplace, which can be done through a new default setting. *See* Apple, "Alternative distribution user experience."

app store and the apps it hosts will be checked for malware and other security threats, manually reviewed by a human prior to distribution, and be subject to the same enhanced on-device security measures as the App Store, including install-time checks and automatic disabling if malware is detected after installation.[25]

The hurdles in the installation process will likely act as a practical deterrent and steer users towards Apple's App Store, which requires no such steps for users to access and utilise it.[26] Furthermore, Apple's App Store will remain pre-installed, prominently displayed, and initially set as the default app store (though the latter can now be changed). The ability to attract users is particularly critical on multi-sided platforms, such as app stores, which have significant network effects. Unless alternative app stores can attract sufficient users *and* app developers, these stores will struggle to even "get off the ground" – let alone grow to exert sufficient competitive pressure on Apple's App Store.

Apple's new approach to enabling alternative app distribution is not far off that of Google in the Android ecosystem. While, in theory, Google permits installation through third-party app stores and browsers on Android devices, Google discourages it by erecting a series of user-facing "scare" screens and mandatory Settings changes, which warn users about the potential harm of "unknown sources." In its recent legal battle with Epic Games,[27] Google justified these additional "security" measures by claiming that alternative sources have higher rates of malware and present a higher risk of a user's device being compromised. However, Epic's security expert, Professor James Mickens,[28] debunked these arguments as pretextual, because the warning screens are not based on any security evaluation of the app-to-install.[29] He further concluded that for the operating system-imposed installation friction to be justified from a security perspective, it "should be proportional to the likelihood that the app is harmful (as determined by a high-quality security review)."[30]

Implications for SMS firms and third parties

It is clear from the above that to justify their security measures, platforms that face SMS investigations need to demonstrate the objectivity of their baseline review standards, as well as the strict necessity of any steps they take to obstruct the users' ability to download apps from third-party sources. If these measures are truly distribution channel-agnostic, there should be no justification for imposing hurdles on installation through alternative sources, especially if the same hurdles are not equally applied to Apple's or Google's proprietary app stores.

Business users, including developers and alternative app stores, also have the potential to play a significant role in providing valuable insights to the CMA – both for the CMA's SMS investigation as well as for conduct requirements.

---

[25] See Apple, "Notarization for iOS apps," https://developer.apple.com/support/dma-and-apps-in-the-eu/#payment-options and "Complying with the Digital Markets Act: Apple's Efforts to Protect User Security and Privacy in the European Union, " https://developer.apple.com/security/complying-with-the-dma.pdf, p.8., March 2024.

[26] In addition, a developer's ability to distribute a third-party app store relies on meeting a set of criteria and obtaining final approval from Apple. These criteria include the establishment of an independent review process, separate from Apple's notarization, to vet apps for intellectual property infringement. Additionally, developers must have the infrastructure to identify and mitigate harmful apps within their stores. Therefore, despite not permitting alternative review entities to vet and approve apps for distribution, Apple mandates developers to implement their own quasi-app review processes as a prerequisite for obtaining the final approval to distribute their app stores on the web. The resulting stringency and lack of flexibility may pose a further barrier for developers of third-party app stores, potentially limiting their ability to enter and innovate. See Apple, "Requesting the entitlement."

[27] See United States District Court, Northern District of California, MDL case no. 21-md-02981-JD; Member case no. 20-cv-05671-JD.

[28] James Mickens is a Professor of Computer Science at Harvard University. *See*: James Mickens (harvard.edu).

[29] Law360, "Epic and Google Security Experts Battle In App Antitrust Trial," November 2023.

[30] The Verge, "Epic's mobile security expert thinks Google should change its app store," November 2023.