

Issues With and Potential Clarifications for the Digital Markets Act

Juan Camilo Castrillón Davis

Abstract— Apple is facing steep fines for its lack of compliance with DMA guidelines. The commission claims that the under the DMA Apple is not adhering to their pro-competition market practices and restricting user choice. This begs the question of what is “strictly necessary” for Apple to enforce on its end, and how the EU will balance the idea of choice in digital markets with rigid methods of user protection.

Keywords—gatekeepers, third-party, side-loading, encryption, ex-ante

I. IN DEFENSE OF APPLE

The Digital Markets Act (DMA) has cornered Apple into making an impossible decision for their company under the pressure of the European Union. The implications of features like allowing side-loading applications, allowing third-party marketplaces, and increasing user data portability raise concerns over the quality of privacy and security that can be maintained [1].

Apple has long been a leader in user data security, and they have done this through their tight control on user data collection; collecting as little as possible and sandboxing apps so that it is hard for apps to access sensitive information on the hardware and even other apps [2] [1]. In adapting to fit the DMA, they have created innovative solutions to protect its users through practices like Notarization and App Reviews, which overall reduce security, but still provide a crucial line of defense [1]. These practices provide a safety net for consumers to not have to worry about what they are downloading through rigorous human detection of social engineering malware, and automated review of known malicious codes. Some threats are too technical for the average user, which makes this process crucial for maintaining security.

Privacy has also been a pillar of Apple’s user experience. Their integrated, closed ecosystem has created a fortified network that people rely on to store lots of sensitive information [1]. With the allowance of third-party marketplaces and side-loaded apps, Apple can no longer provide the rigorous standard of protection offered through its App Store guidelines, which exposes users and developers alike to potential harm in the form of sub-par content regulation and a less intuitive experience [3]. A core principle of Apple’s design is “to make sure users know what data of theirs is being shared and how it is used, and that they can exercise control over it” [1]. Users will not have the same transparency when dealing with third-party services, which is a significant, unnecessary increase in the burden on users to protect their data with less information.

Apple is working well within its means provided by the DMA to uphold pro-competition practices within an EU digital marketplace. It has created new tool kits for developers to assist them in integrating alternative methods of payments and easing control over access to embedded websites [2]. They have also created easy modes of downloading their signed (verified) binary for portability to different marketplaces, giving them more choice on where they would like to sell their goods [4]. It is not fully Apple’s place to regulate maximum competition in the market, but they do have responsibility to facilitate options for their users safely just like any other company. Providing choice to developers and users on where they practice business, while maintaining sufficient privacy standards is a fine balance that Apple is continuing to collaborate with the commission on reaching.

II. IN DEFENSE OF THE COMMISSION

The DMA provides a strong, pro-consumer regulation standard that benefits European users through providing more choice, regulatory advantage to the government, and increasing data rights to business users [5]. Through these principles, the commission is offering a different perspective on the balance between user security and privacy and ensuring antitrust enforcement.

One of the biggest issues faced by regulators today is the ever-evolving, fast-paced industry that technology has become. This has made it even more difficult to apply competition law to digital markets [6]. The DMA finally gives regulators at least an even footing with its ex-ante (prevention) approach to legislation. It simplifies the process for enforcement with standardized classification of gatekeepers and practices they must uphold through articles 5-7 of the document [7]. This instant obligation to comply with practices such as side-loading, third-party facilitation, and interoperability creates an easier method of ensuring pro-competition practices among the largest gatekeepers without a hard-to-prove evidence-gathering nature of current legal cases.

Moreover, privacy concerns do not just take the form of data collection. Data management is just as important of an issue, and the DMA dramatically improves this through data portability and interoperability mandates. These mandates allow users more options for how to manage data on their own, which includes finding different services that might fit their privacy preferences better [6]. It also prevents gatekeepers from combining personal data across platforms without proper consent [5], which prevents unknown data sharing and

processing for users. Centering the methods of privacy around user autonomy over data instead of collection of user data helps users freely store and share their data as they please and not be locked into heavily integrated systems like Apple's.

When it comes to protecting users' data, the DMA provides guidance and requirements on the basic needs for this new world of interoperability. Article 7 of the DMA includes provisions to create a standard of end-to-end encryption for interoperability between sites and apps [8]. This baseline of proven security methods helps provide an overarching safety net for this world of streamlined data control and connection between businesses. When interacting and using gatekeepers, this even extends to third parties needing to meet minimum requirements for security under that very same article [8].

III. SUGGESTIONS TO THE CHAIRMAN

Mr. Chairman, it is my opinion that you should lean on the side of Apple in your stance on this issue. There are several issues that stand out in the DMA that need to be addressed before this regulation can be properly and equally enforced for the benefit of EU citizens. One of my key concerns with the DMA is its clarity on the issue of how to manage gatekeepers like Apple who have legitimate concerns over the security of their hardware.

The DMA currently states under article 10 that a gatekeeper may be exempt from DMA compliance "on the grounds of public health or public security" [7]. With the widespread use of Apple devices throughout Europe, the DMA's streamlining of data sharing and opening of gatekeepers' privacy and security practices exposes the EU users to more threats. This document's preventative approach, while it succeeds in providing us with the preventive measures for anti-trust, expands the surface area of preexisting systems and allows for more potential points of vulnerability for user data.

Apple's addressing of the issue through the implementation of Notarization and App Review are good mediums for maintaining polished standards of security while upholding pro-competition mandates from the DMA. They offer choice to developers and users on what they can use to buy, sell, and create apps safely, without putting undue burden on users to vet every single app they encounter [1].

The friction that Apple has encountered is in large part due to vagueness in critical wording of the DMA. Specifically in

Article 6 it states that a gatekeeper "can take strictly necessary and proportionate measures to ensure that a third-party app (store) does not endanger the integrity of its operating system or hardware or to enable end users to effectively protect security" [7]. The idea of strictly necessary is not defined enough to create clear guidance on adaptation for companies nor enforcement for regulators.

In conclusion, Apple's practices, although not as open as the Commission would like, should be considered with the benefit of the doubt. The best path to advocate lies in creating more precise wording in the DMA on what is considered "proportional and strictly necessary," and furthermore, you can call for steps to be taken in terms of more rigorous auditing of gatekeepers to ensure that practices like Apple's are indeed being used for their intended purposes.

REFERENCES

- [1] JG. Davis, "Complying with the Digital Markets Act: Apple's Efforts to Protect User Security and Privacy in the European Union Complying with the Digital Markets Act," Mar. 2024. Accessed: Jul. 07, 2025. [Online]. Available: <https://developer.apple.com/security/complying-with-the-dma.pdf>.
- [2] "Apple's DMA Compliance Report Non-Confidential Summary," Apple, Mar. 2025. Accessed: Jul. 07, 2025. [Online]. Available: <https://www.apple.com/legal/dma/NCS-March-2025.pdf> K. Elissa, "Title of paper if known," unpublished.
- [3] "Apple's Non-Confidential Summary of DMA Compliance Report," Apple, Nov. 2024. Accessed: Jul. 07, 2025. [Online]. Available: <https://www.apple.com/legal/dma/NCS-October-2024.pdf>
- [4] "Apple's Non-Confidential Summary of DMA Compliance Report," Apple, Mar. 2024. Accessed: Jul. 07, 2025. [Online]. Available: <https://www.apple.com/legal/dma/dma-ncs.pdf>
- [5] L. M. B. Cabral, J. Haucap, G. Parker, G. Petropoulos, T. M. Valletti, and M. W. Van Alstyne, "The EU Digital Markets Act: A Report from a Panel of Economic Experts," *papers.ssrn.com*, Feb. 09, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783436 (accessed Jul. 07, 2025). M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [6] T. Papadopoulos and Louiza Kofina, "Digital Markets Act: A promise for a fairer digital environment or a failed experiment?," *SSRN Electronic Journal*, Jan. 2024, doi: <https://doi.org/10.2139/ssrn.4997075>.
- [7] N. Moreno Belloso, "The EU Digital Markets Act (DMA): A Summary," *SSRN Electronic Journal*, 2022, doi: <https://doi.org/10.2139/ssrn.4109299>.
- [8] Mikołaj Barcentewicz, "How the New Interoperability Mandate Could Violate the EU Charter," *Lawfare*, 2023. <https://www.lawfaremedia.org/article/how-the-new-interoperability-mandate-could-violate-the-eu-charter> (accessed Jul. 07, 2025).