Living Dangerously:

The DMA and the Challenge of Balancing Competition and Cybersecurity

Giuseppe Colangelo

Jean Monnet Professor of European Innovation Policy and Associate Professor of Law and Economics, University of Basilicata

11 March 2025

Summary

- Risks to platform integrity and security are emerging as significant concerns in the implementation of the Digital Markets Act (DMA).
- Since policymaking involves trade-offs, the European Commission should assess whether the solutions proposed by gatekeepers align with the goal of fostering competition while maintaining an adequate level of security, ultimately achieving a constrained optimum.
- When evaluating gatekeepers' technical implementations, it is crucial to account for the substantial differences in their business models.
- Due to information asymmetry between regulators and targeted companies, achieving a proper balance between competition and security requires the active involvement of gatekeepers.
- The experience of initiatives like Open Banking demonstrates that it is possible to promote competition without compromising security.

Table of contents

About the author

Giuseppe Colangelo is an Associate Professor of Law and Economics at University of Basilicata (Italy). He also serves as Adjunct Professor of Markets, Regulation and Law at LUISS (Italy). He is a fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum (TTLF), the scientific coordinator of the Research Network for Digital Ecosystem, Economic Policy and Innovation (Deep-In), and an academic affiliate with the International Center for Law & Economics (ICLE).

About EPICENTER

EPICENTER, the European Policy Information Center, is an independent initiative of twelve leading think tanks from across Europe. It seeks to inform the European policy debate and promote the principles of a free society by bringing together the expertise of its members.

EPICENTER is formed by the Center for Political Studies (Denmark), Civil Development Forum (Poland), Fundalib (Spain), the Institut economique Molinari (France), the Institute of Economic Affairs (UK), the Institute of Economic and Social Studies (Slovakia), the Institute for Market Studies (Bulgaria), Istituto Bruno Leoni (Italy), KEFiM (Greece), the Lithuanian Free Market Institute, Prometheus (Germany), and Timbro (Sweden). Like its members, EPICENTER is politically independent and does not accept taxpayer funding.

Introduction

As the Digital Markets Act (DMA) enters its implementation phase, the European Commission is investigating whether the proposed solutions of dominant tech firms (gatekeepers) comply with the mandates of the DMA. However, this process is unearthing new concerns about potential side effects and unintended consequences. One such concern is that pro-competition measures could weaken platform integrity and security, exposing end users to data breaches, scams, and privacy risks. Further, the topic is highly sensitive due to its potential geopolitical implications.

However, this debate is inevitable, as DMA mandates aim to promote fair access by opening up gatekeepers' ecosystems, particularly app stores. The requirements include supporting sideloading (letting users install apps outside the app store), interoperability requirements (requiring smooth integration with third-party services), and obligations to remove anti-steering restrictions (allowing businesses to directly communicate with end users, promote offers, and enter into contracts with them, without going through the gatekeeper).

Against this backdrop, to mitigate the growing risk of polarisation – which has at times affected even academic discussions – it may be useful to identify common ground and outline reasonable principles to guide policymakers in addressing these complex challenges.

Navigating trade-offs: primary rationales and safeguards

We need to start by acknowledging that policymaking is fundamentally about trade-offs. This means that binary choices and appeals to a singular 'greater good' are ineffective. Policymaking is the art of balancing conflicting yet relevant interests. Therefore, policymakers should not favour one objective at the expense of another. It would be equally unacceptable to enhance competition by disregarding security risks or, conversely, prioritise consumer protection while neglecting the need for competition.

How policymakers strike this balance depends on the weight regulatory interventions assign to each of the interests involved. To this end, it is essential to distinguish between the primary rationales driving a policy intervention and the safeguards that constrain its scope.

In the case of the DMA, it is unquestionable that the primary goal is to promote competition in digital markets. At the same time, user security must be safeguarded. Accordingly, gatekeepers are not prohibited from adopting necessary and proportionate measures that ensure the integrity of their services and end users' security. Similarly, in its recent landmark *Android Auto* decision, the Court of Justice held that, under antitrust law, a dominant player is obliged to grant third parties equal access to the platform and ensure interoperability when the platform – by its nature and business model – has been designed to enable third-party undertakings to operate on it. However, this obligation does not apply in cases of technical impossibility or where access would harm the platform's integrity or security.

Against this background, policymakers must seek solutions that achieve a constrained optimum, which safeguards against potential risks, rather than an unconstrained optimum. This means that, as a first guiding principle, when assessing the solutions proposed by gatekeepers for DMA compliance, the European Commission should not aim for the highest possible level of competition in absolute terms. Instead, it must seek the highest achievable level of competition while also ensuring an appropriate degree of security.

The role of business models

In this context, a second key consideration is the differences in gatekeepers' business models. The platform's business model will significantly influence its strategies and incentives. Moreover, a business model perspective will help to account for the role of platform design and governance in value creation. Indeed, due to the inherent dualism of multi-sided markets, the same economic factors that drive ecosystem growth can also pose significant risks to their success. Striking a delicate balance is essential to ensure that the ecosystem remains viable and does not discourage specific user groups from engaging with the platform. Notably, platform ecosystems are highly vulnerable to negative externalities, since the value created is not entirely under the platform's control, but depends on the participation and actions of users. Thus, governance plays a crucial role in an ecosystem's success. This is why platform owners regulate access to and interactions within their ecosystems to preserve value and platform integrity.

However, the DMA has been drafted with a business model–agnostic approach. Gatekeepers are subject to the same obligations regardless of their business model.

Nonetheless, in implementing the DMA and assessing tech companies' solutions, the Commission should consider the business context in which these measures will be implemented. This, in turn, will help it evaluate whether the proposed solutions will aid in achieving a constrained optimum – namely, fostering competition while ensuring an adequate level of security.

More specifically, both Apple and Google have raised security concerns in their compliance reports, emphasising the significant investments they have made to build user trust in their respective app-store ecosystems. When evaluating their technical solutions – particularly regarding anti-steering restrictions as well as sideloading and vertical interoperability requirements – it is essential to consider the significant differences between their business models and how users access their respective mobile ecosystems.

Building on the foregoing analysis, I argue that the balance between competition and security cannot be the same in a closed ecosystem as it is in an open one. Indeed, the DMA's pro-competition goal is particularly challenging to achieve in the case of Apple's mobile ecosystem, which is often described as a walled garden due to its tightly integrated and closed architecture.

The devil is in the (technical) details

A third key consideration is that DMA compliance should be viewed as a two-way street, where all parties cooperate and contribute to finding appropriate and reasonable solutions. So, while the previous two points were directed at the Commission, it is also important to emphasise that a balance between competition and security cannot be achieved without the contribution of gatekeepers. This is particularly relevant when implementing obligations that require technical interventions, as such cases highlight the stark information asymmetry between enforcers and the targeted companies, which cannot be bridged without the aid of the companies themselves.
In this context, and in line with my initial warning against binary choices, it would not be possible to have a productive discussion if security risks are over-prioritized vis-à-vis competition and used to completely neutralise the effects of DMA obligations. This would distort the balance between the DMA's primary goal and its safeguards. Similarly, dominant firms must not be allowed to invoke security and privacy concerns as a shield to protect themselves from the enforcement of pro-competition rules.

Therefore, it is the responsibility of gatekeepers to develop technical solutions that reconcile the dual need for competition and user security. In turn, the Commission must remain open-minded and be willing to consider the specific features of each proposed solution.

The European Open Banking experience provides a valuable example. By requiring banks to grant third parties secure access to user data at the customer's request, the initiative empowers individuals to take control of their financial information. The EU was one of the first jurisdictions to make Open Banking mandatory by introducing the access-to-account rule, which requires banks to provide customer account data to all authorised third-party payment service providers and execute payment orders.

From the beginning, the initiative was guided by the objective of raising competition. In this scenario, the legacy banks were the gatekeepers. However, alongside the benefits that came with increased competition, there were also risks, as Open Banking potentially exposed consumers to privacy and security harms. To address this, a strong customer authentication system was introduced, requiring two-factor authentication based on either knowledge (e.g., a password), possession (e.g., a card), or inherence (e.g., a fingerprint). A recent evaluation report published by the Commission concludes that this measure has been successful in reducing fraud.

I'm not suggesting a technical comparison between Open Banking and DMA measures to ensure consumer protection against security risks. Furthermore, I'm not suggesting that it would be easy to define technical security standards under the DMA to guarantee an appropriate level of protection. I'm simply noting that Open Banking faced similar security concerns, and its experience demonstrates that solutions can be found to promote competition without compromising security.

Competition or security, that should not be the question

The revival of regulation has sparked an intense debate about the value of this type of intervention compared to traditional antitrust enforcement. Many voices have highlighted the potential downsides of (over)regulation, arguing that the risks in terms of side effects and unintended consequences may outweigh its potential.

In this context, security risks are a particularly sensitive issue for policymakers, as it would be challenging to justify that it is worth pursuing openness in digital ecosystems at the expense of end-user protection.

Consistent with my initial proposition, this brief contribution serves as a call against polarised approaches and an invitation to embrace the challenges of managing trade-offs. This is unavoidable for entities like the EU, which have chosen to intervene in digital markets through regulatory initiatives.

References

CJEU, 25 February 2025, Case C-233/23, *Alphabet and others v. Autorità Garante della Concorrenza e del Mercato*, EU:C:2025:110.

European Commission, *Report on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market*, COM(2023) 365 final.