

**Question for written answer E-004795/2025
to the Commission**
Rule 144
Piotr Müller (ECR)

Subject: Digital security and competition requirements under the Digital Markets Act (DMA)

The Digital Markets Act (DMA) was developed to strengthen competition and limit harmful practices by the largest technology companies.

Fair competition promotes innovation and the development of a single digital market. In its efforts to enforce platform openness, in particular through Article 5(4), the Commission requires operating system providers to allow uncertified third-party applications. Experts warn that this could undermine the integrity of security architecture and expose users to a greater risk of cyberattacks, including phishing and malware infections.

Paradoxically, instead of improving competition, the enforced changes may weaken it in the area of mobile systems, while also reducing the quality of services¹.

The lack of direct access to integrated functions – such as map applications from the search engine – makes it difficult to use basic tools that were previously convenient and widely available.

In view of this situation:

1. On what evidence did the Commission base its decision to prioritise regulatory requirements over cybersecurity risks?
2. Who will be held responsible if the systemic changes forced by the DMA lead to breaches of users' device and data security?
3. Does the Commission feel that limiting 'self-preferencing' is more important than ensuring that users can use digital services safely and conveniently?

Submitted: 3.12.2025

¹ <https://ecipe.org/blog/dma-gift-to-hackers-threat-to-competition/>