ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

NEWS – ECIPE PRESS RELEASE – NEW POLICY BRIEF

Cybersecurity at Risk: How the EU's Digital Markets Act Could Undermine Security across Mobile Operating Systems

By **Matthias Bauer** *and* **Dyuti Pandya,** *Director and Analyst at ECIPE*

Brussels, 17 February 2025 - The European Union's Digital Markets Act (DMA) is at risk of compromising cybersecurity by forcing mobile operating system (OS) providers to open their platforms to unregulated third-party app distribution channels. Specifically, **Article 5(4)** may require providers to weaken or bypass built-in security protocols, increasing exposure to malicious software, phishing attacks, and data breaches.

"We have long warned that the DMA's vague and often contradictory provisions could create more problems than they solve. Instead of fostering clarity and fair competition, it has left businesses and consumers facing legal uncertainty and confusion over market access in the EU. Recent developments have only reinforced these concerns," said Matthias Bauer, lead author of the Policy Brief.

The unintended consequences of the DMA are already materialising. Apple has opted to withhold advanced security enhancements and AI-driven features from EU users, citing compliance risks. Similarly, Android, an open source OS, could be forced to dismantle key elements of its security architecture, reducing its ability to protect users, developers, and manufacturers reliant on its ecosystem.

"The application of the DMA should be technology-neutral, allowing different ecosystem models to compete while ensuring strong security standards," Bauer continued. ***"Operating system providers are best positioned to assess and block malicious apps, safeguarding user trust and platform integrity."***

To ensure security is not sacrificed in the name of competition, EU policymakers should now:

- **Ensure Technology Neutrality** – The DMA should recognise diverse platform architectures rather than enforcing a one-size-fits-all approach.

- **Uphold Regulatory Coherence** – DMA enforcement must align with EU cybersecurity frameworks such as NIS2 and the Cyber Resilience Act (CRA) to avoid regulatory contradictions.

- **Recognise Platform Differences** – Competition policy should reflect the unique security needs of different operating systems rather than imposing uniform requirements.

- **Preserve Security Measures** – OS providers should retain the ability to block unvetted links while implementing verification mechanisms for external links where necessary.

- **Exempt Justified Security Actions** – When facing evidence-based cybersecurity threats, OS providers should not be penalised for enforcing essential security measures.

Publication details: Cybersecurity at Risk: How the EU's Digital Markets Act Could Undermine Security across Mobile Operating Systems, ECIPE Policy Brief No. 05/2025,

Contact the corresponding author: Matthias Bauer, matthias.bauer@ecipe.org

Media inquiries: info@ecipe.org or +32 2 289 13 50