CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

EUROPE'S DMA:

A Cybercriminal's Paradise?

By Heather West, Senior Fellow, Center for European Policy Analysis, Senior Director Venable LLP

DECEMBER 2025

Table of Contents

The Digital Markets Act mandates that the largest digital platforms allow interoperability — overlooking the security dangers.

This report originally appeared as a short series of articles on CEPA.org

Introduction

Mobile devices serve as wallets, medical portals, and workplace IDs. A single vulnerability in the operating system can expose financial information, health data, or corporate credentials. When rules that aim to promote competition inadvertently weaken these defenses, the effects are felt not only by platform providers but by every user.

This paper focuses on the implications of DMA provisions around interoperability of hardware and software on mobile operating systems, identifies the key risks, and makes recommendations to avoid weakening the mobile ecosystem. Article 6(7) of the DMA requires designated "gatekeepers" to provide developers and businesses with free and effective interoperability with mobile hardware and software, including those features controlled by the operating system (OS). While intended to promote competition, the mandate requires operating systems to open internal functions in ways that disrupt security protections. They open a wide attack surface, threaten data integrity and confidentiality, increase system instability, create vulnerabilities in authentication and authorization, and erode user privacy.

User trust has been a cornerstone of mobile adoption. The security and privacy assurances provided by integrated mobile operating systems have enabled widespread adoption of sensitive services such as mobile payments, health applications, and enterprise productivity tools. If interoperability mandates erode that trust, consumers may become reluctant to adopt new services or may disable interoperability features altogether. Instead of promoting competition and innovation, poorly implemented interoperability could stifle uptake of alternative services. Preserving user trust should be seen as an integral part of achieving the DMA's pro-competition objectives.

Secure mobile operating systems already have sophisticated interoperability capabilities – openness and interoperability are not necessarily in tension. But measures to achieve a level playing field and competition in the digital market must not trample security by compromising existing system design. And if users distrust their mobile devices, it will negatively impact the mobile market.

DMA interoperability is difficult to implement. Modern mobile operating systems are designed to control and limit access to the core functions of the operating system.

A central objective of the DMA is to enhance competition and contestability — the ability of rivals to challenge dominant firms by lowering switching costs and reducing lock-in.

The Commission designates gatekeepers as platforms that function as important gateways to end users and hold entrenched or durable positions. To date, the European Commission has named 23 core platform services from seven companies: Alphabet, Amazon, Apple, Booking, ByteDance, Meta, and Microsoft.

The DMA does include a security clause allowing gatekeepers to adopt "strictly necessary and proportionate" measures to preserve the integrity of their services. But this qualifier offers limited practical protection. Policymakers can deem security safeguards to be excessive or unjustified.

Device manufacturers or operating system developers can claim security risks that are unlikely to manifest. Firms requesting interoperability can dismiss real security risks. Admittedly, gatekeepers also can use the security opt-out to resist safe changes.

The result is a potential erosion of the trust that users place in mobile platforms.

Competition concerns are valid and should be addressed — but surely competition and contestability can be improved while maintaining the advances that mobile devices have brought to our collective cybersecurity.

The mobile integrated model stands in deliberate contrast to traditional desktop systems such as Microsoft Windows or Linux, where early architectural decisions toward open interoperability with third-party hardware and software fostered innovation. This same openness created persistent vulnerabilities, resulting in malware proliferation, driver conflicts, and fragmented updates.

Mobile operating systems were designed and refined to avoid those weaknesses by emphasizing integration and restricting access to core functions. Modern mobile operating systems rely on layered or 'tiered' security, similar to airport checkpoints. Both Apple's iOS and Google's Android use tiered access permissions. Apps and services must pass through multiple verification gates — such as sandboxing, permission prompts, and OS-level authentication — before they can interact with sensitive hardware or data. Each layer catches what another might miss, creating predictable and controlled pathways. Mobile operating systems retain privileged control over core functions such as software updates and hardware interactions, while third-party apps require permission to be installed.

This permission system limits opportunities for hacking, but also limits, by design, access for untrusted applications or developers. The Apple App Store and Google Play Store vet apps for malware or risky functionality.

Similar limitations and controls are in place throughout the device and operating system, though less visible to the user. This provides defense-in-depth — multiple layers of protection, such as hardware-based security, encryption, permission controls, and secure boot processes. Even if one control fails, others remain in place to prevent compromise.

Unavoidably, interoperability mandates to disrupt this integration — including Article 6(7) — present significant tensions with the design of mobile operating systems. The history of computing is full of examples where efforts to make systems more open or compatible also made them more vulnerable. Key risks and technical challenges, discussed in part two of this series, illustrate these tensions.

Opening Up: Europe's DMA and the Risks of Interoperability

Modern mobile operating systems are designed with integrated security architectures that limit malicious access, carefully managing connections between hardware, software, and apps. The DMA's hardware and software interoperability mandate, Article 6(7), requires designated "gatekeepers" to provide developers and businesses with free and effective interoperability with mobile hardware and software features, including those features controlled by the operating system.

Key Risk: Expanded Attack Surface

Interoperability mandates introduce new entry points that malicious actors can target, expanding the attack surface and increasing security risks. Importantly, these entry points were likely not considered when the operating system (OS) was developed, meaning that the security architecture does not take these new targets into account.

The newly exposed interfaces increase the risk of direct memory access attacks, in which an attacker gains access to and directly manipulates the computer's memory. Modern operating systems limit access to memory because these attacks can bypass almost any other security protections — direct memory access gives an attacker the keys to the kingdom. They can plant spyware, bypass permission limitations, change stored data, remove password requirements, extract encryption keys, escalate privileges, or install a system backdoor without interference.

The Pegasus spyware is one example of the consequences of expanded attack surface; it uses OS-level access to reach cameras, microphones, and messages through hidden system interfaces that were not designed to be used by non-system apps. When the security layers protecting a device are exposed, even a small vulnerability can expose the entire phone.

Key Risk: Data Integrity and Confidentiality

There are also risks to data integrity and confidentiality without direct memory access. In submitting interoperability requests, developers can request access to broad types of data. Although not necessarily malicious, overly broad access to user data can risk user privacy and security. Additionally, access requests may be intentionally vague or broad to sidestep permissions for certain kinds of data, like notification content, Wi-Fi history, or message history. It is not yet clear whether the DMA will be interpreted as eliminating permissions for this sensitive content, or if there is an "equally effective" way to grant access to legitimate developers, but it is a growing concern surrounding initial requests for interoperability. Legitimate actors may ask for overbroad access, and malicious actors might abuse DMA mandates to harvest or misuse certain personal data by asking for interoperability and bypassing the permission architecture in place.

Interoperability requests that replicate the overbroad permissions of past data-sharing systems risk repeating failures like Cambridge Analytica, where a seemingly harmless quiz app collected millions

of users' personal details through an open Application Programming Interface (API) and shared them without consent.

Similar issues have occurred on Android, where malicious apps misused the accessibility service — intended to help people with disabilities — to read messages and capture passwords. Giving third parties wider access to data, even for good reasons, can quickly spiral into privacy abuse when oversight or limits are weak.

Key Risk: System Instability and Degraded Performance

In July 2024, CrowdStrike implemented an anti-virus update that crashed computers around the world. The CrowdStrike product had access to the kernel, deep in the operating system, and the misconfigured file impacted the operating system and memory access. Mobile phones emerged unscathed thanks to their secure architecture relative to PCs.

Mobile operating systems rely on centralized control and vertical integration. They are not engineered for arbitrary third-party integrations. Disruptions to this architecture put the stability of the system at risk and could cause system crashes, degraded user experience, and delays in innovation.

Consider, for example, Apple's AirDrop or Google's Nearby Share, both designed as seamless and secure file-sharing tools within trusted boundaries and with security controls. If Article 6(7) compels these services to interoperate with third-party file-sharing apps or hardware, without equivalent safeguards like malware scanning, robust encryption, and strict performance controls, the result could be a dramatic increase in system instability and security risks.

Key Risk: New Supply Chain Vulnerability

In 2019, foreign threat actors targeted the US federal government and private sector entities in a widespread campaign that became known as SolarWinds. To accomplish this unprecedented breach, the attackers executed a supply chain attack, infiltrating a third-party software vendor's network and imbedding malicious code to be shipped to the vendor's customers without their knowledge.

Supply chain attacks can have widespread impact across all types of downstream organizations and are difficult to detect. Mobile operating systems benefit from a multi-layered defense-in-depth strategy, which fortifies them against supply chain attacks. Unvetted components from third parties can compromise their integrity. When a third-party component is compromised, it becomes an attack vector.

One-size-fits-all regulation undermines differentiated security models. In part one of this series, I outlined the high-level architecture that mobile OSs share, but further differences exist in their security models. Interoperability mandates that do not take differentiated security models into account can have even greater unintended consequences, making simplistic assumptions about how security controls are implemented and forcing new architectures into established computing

systems. This is like a mandate that all doors have security guards in front of them, instead of allowing a guard, a security monitoring system, or a deadbolt to accomplish the same goal.

Key Risk: Authentication and Authorization Weaknesses

Mobile operating systems mitigate security risks through identity verification and access control, but third-party access at the operating-system level complicates this. While identity verification for apps is used to manage an account, authentication at the OS-level is the basis of a device's trust model. Instead of logging into an app or service, hardware and operating system authentication establish who can control the device itself. If this is bypassed or compromised, every app and all the device's data are vulnerable.

Modern mobile operating systems increasingly rely on hardware-backed authentication mechanisms, such as Apple's Secure Enclave or Android's Trusted Execution Environment, because software-based security has not proven adequate. These modules provide tamper-resistant storage of cryptographic keys and enable device-level identity verification. Interoperability mandates that compel third-party access to operating systems or hardware features may bypass or dilute these protections by requiring tokens or credentials to be shared. This weakens the principle of least privilege — the idea that any user or program should have the least permissive access necessary to accomplish a task — and creates new opportunities for impersonation to apps or services.

Key Risk: Technical Challenges

Certain technical challenges arise from the tension between open access and secure design. Once systems become heterogeneous, the engineering complexity increases exponentially.

Engineering secure interoperability across complex, vertically integrated operating systems introduces exponential complexity. Each additional integration layer — whether for translation, backward compatibility, or hardware abstraction — creates new code paths that must be tested, patched, and maintained. This complicates vulnerability management and increases the likelihood of regressions in performance or stability. Moreover, because third-party components may evolve independently, the task of maintaining a coherent security baseline becomes significantly harder for OS providers. Rigid compliance deadlines imposed without regard to this complexity risk forcing unstable implementations into the market. The DMA imposes interoperability in ways that outpace security governance capacity.

DMA interoperability obligations also interact with the broader EU regulatory landscape. The Network and Information Security Directive (NIS2) imposes cybersecurity risk management and reporting obligations on operators of essential and important entities. The General Data Protection Regulation (GDPR) requires data minimization and strict safeguards for personal data processing. The Cyber Resilience Act (CRA) sets baseline security requirements for connected devices and software. Some requests for interoperability under the DMA already implicate multiple frameworks — for example, access to Wi-Fi history implicates data protection and cybersecurity equities.

Under these parallel frameworks, gatekeepers may face conflicting obligations — for example being required to allow access to sensitive data or APIs under the DMA while simultaneously being liable for breaches under NIS2 or GDPR. Coordinating the DMA with these regimes and providing clarity to gatekeepers about their obligations is essential to avoid undermining Europe's broader cybersecurity and privacy protections.

Making Interoperability Work: Recommendations for Europe's DMA

The architectural reality of mobile operating systems creates an unavoidable tension between open access and secure design, complicating the implementation of the DMA's interoperability mandate. That need not be the case.

To conclude Europe's DMA article series, I offer a set of recommendations for secure implementation of Article 6(7).

- **Interpret "effective interoperability" in terms of outcomes, not privileges:** The European Commission should clarify that Article 6(7) guarantees equivalent functional access for third parties but does not require identical internal entitlements to OS-private or kernel-level interfaces. For example, similar outcomes can be achieved using secured and scoped APIs for access to virtual assistant, hardware, or software features.

- **Establish a tiered access model for interoperability features:** Gatekeepers should be required to implement a three-tier risk model (low, moderate, and high-risk) for new interfaces, with escalating obligations for each type of interface. This operationalizes Article 6(7)'s security safeguard in a predictable way. Low-risk interfaces, such as those without persistent privileges, could be presumed allowable to all registered developers. Access to security-sensitive features or hardware should be contingent on additional controls for developers that seek to access these features, data, or APIs.

- **Require security impact assessments before new interoperability features are implemented:** Policymakers should mandate a formal security impact assessment (SIA) for each Article 6(7) interface before it is activated, including an assessment of whether the interface poses low, moderate, or high risk to user data and security. These assessments should include potential unintended consequences on the security and privacy of users, threat modeling, and supply-chain risk mapping.

- **Preserve end-to-end encryption and data minimization by default:** Interoperability implementations must not weaken end-to-end encryption or expand data collection beyond what is strictly necessary. Each interoperability API should include a data-minimization statement and a privacy threat model.

- **Align DMA enforcement with evolving cybersecurity standards and timelines:** The Commission should align interoperability guidance with established EU cybersecurity frameworks (e.g., NIS2, ENISA risk models) and reconcile compliance timelines with technical feasibility. The Commission should work in an interagency fashion with their cybersecurity and privacy counterparts on interoperability determinations. Additionally, enforcement deadlines should be staged and extendable based on results of security impact assessments, and security testing.

- **Involve ENISA in evaluating the cybersecurity implications of interoperability requests:** The European Union Agency for Cybersecurity (ENISA) should play a formal role in reviewing the security aspects of interoperability requests and proposed implementations under Article 6(7). ENISA's technical expertise and risk-assessment methodologies can help assess whether proposed interoperability features introduce unacceptable cybersecurity or privacy risks, and whether proposed implementations are sufficiently protective. By consulting ENISA on security impact assessments and during enforcement decisions, policymakers can ensure that interoperability requests are measured against consistent technical criteria and informed by current threat intelligence, rather than by business or political considerations alone. This coordination would also help harmonize DMA implementation with the EU's broader cybersecurity strategy and frameworks under NIS2 and the Cyber Resilience Act.

Policymakers' efforts to ensure market competition and platform providers' efforts to ensure the security of their operating systems are not mutually exclusive. Interoperability mandates must account for the architectural realities of modern operating systems, — particularly mobile operating systems. Competition goals and cybersecurity imperatives must be acknowledged and reconciled.

If policymakers want to avoid undermining user trust, safety, and system stability, they must collaborate with platform providers and developers to ensure that architectural and security realities are understood and considered. As it stands, the DMA imposes interoperability requirements in a way that outpaces security governance capacity, putting platform integrity, user data, and overall cybersecurity at risk.

Article 6(7) should be implemented with security-by-design principles: tiered access, feasibility gates, and transparency mechanisms that preserve operating system integrity while enabling third-party innovation. If implemented with care, the DMA can serve as a model for acknowledging the interplay of competition and cybersecurity in digital markets. By drawing on ENISA's expertise and grounding enforcement in established cybersecurity frameworks, the EU can demonstrate that digital trust and market competition are mutually reinforcing. Europe can set a global model for integrating economic and security policy in the digital age. The path forward is not to dilute either competition or security, but to align them.

About the Center for Cybersecurity Policy and Law (CCPL):

The Center for Cybersecurity Policy and Law is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats. Established in 2017 as a 501(c)(6) nonprofit, the Center combines policy expertise with convening power to bring industry leaders together with policymakers, form coalitions, and launch initiatives that produce real-world outcomes.

About the Center for European Policy Analysis (CEPA):

The Center for European Policy Analysis (CEPA) is a nonprofit, nonpartisan, public policy institution headquartered in Washington, DC, with hubs in London and Brussels, focused on strengthening the transatlantic alliance through cutting-edge research, analysis, and programs. CEPA provides innovative insight on trends affecting democracy, security, and defense to government officials and agencies; helps transatlantic businesses navigate changing strategic landscapes; and builds networks of future leaders versed in Atlanticism.