MEMO

TO: Members of Congress
FROM: Members of ACT | The App Association
DATE: September 10, 2025
RE: Negative Impacts of the Digital Markets Act on Small Business

---

The Digital Markets Act (DMA) severely disadvantages small business innovators, even though its scope is technically limited to large online marketplaces and platforms. It is one policy amid a growing wall of EU regulatory interventions that make it more difficult and more expensive to operate in or access the European market. Other bricks in the wall include the EU's Digital Services Act (DSA), which adds a layer of unnecessary compliance and privacy challenges, and the Artificial Intelligence (AI) Act, which has caused debilitating levels of confusion for startups and small businesses in the app economy.

App Association members struggling under this "culture of compliance," are speaking up about the harms of the DMA with policymakers and peers throughout Europe.

Privacy and Security Challenges

DMA requires smart devices to accept third-party app stores and open access to your device for any device maker or service provider. This circumvents the curation and vetting of mobile apps or connected devices that major platform operators currently do to prevent malware and criminals from getting access to your device or your data. This erosion of security and privacy reduces customer trust in the safety of downloading apps. That loss of trust disproportionately impacts App Association members, which depend on consumers having some level of assurance that apps made by companies they have never heard of are safe and work as intended.

Mitchel Volkering, founder of Netherlands-based Vaic.at: "There is no such thing as perfect security, but I can guarantee that individual smartphone users' privacy and security will get worse if you mandate the existence of additional threat vectors. **You do not deal with a hole in a boat by shooting another hole in it.**"

Clément Sauvage, founder of France-based Bits 'n Coffee: "Smart devices have very sensitive data. They're now repositories of healthcare information, precise location, personal photos, and confidential messages that people do not expect to be shared. DMA's interoperability mandates are being applied to require support for notifications to third-party wearable devices in ways that subvert consumers' expectations. Meta's business model is to make money on my data. I know that, and that's why I don't share information with them. **These mandates would take that choice out of my hands.**"

DMA-Caused Delays

The DMA has built-in periodic reviews in order to assess the impact and address lessons learned about unintended consequences. One of those reviews is currently under way, and unfortunately, rather than signaling changes that would reduce the burden of DMA, the European Commission has talked about expanding it to "the artificial intelligence (AI) sector." The DMA and other European tech regulations have already delayed the introduction of the latest AI models in Europe, forcing small business innovators in the EU to rely on older models and U.S. app companies to build the delays into their products in order to continue reaching EU customers.

Clément Sauvage, founder of France-based Bits 'n Coffee: "EU developers shouldn't be blocked from using tools like Llama 4 and Apple Intelligence. **The delay puts us at a distinct disadvantage against our U.S. and other global rivals,** who get to use the latest technology has to offer. DMA shoots us in the foot in this regard."

Mitchel Volkering, founder of Netherlands-based Vaic.at: "We're restricted from accessing innovative new tools and features that Apple and other companies release in the U.S. and other regions. These include Apple Intelligence and iPhone Mirroring. In the EU, when these tools do arrive, they're often late and degraded versions. **Competing with rivals based outside the EU has never been more challenging than it is today.**"

Sebastian Holst, founder of New Jersey-based Fool Me Once, LLC: "We've already seen how trusted marketplaces convey security and scale to small business offerings, opening markets and fueling growth. Assuring responsible AI raises the stakes and the expectations by orders of magnitude, making the stabilizing and standardizing influence of trusted platforms more important than ever before. I would be hard-pressed to find a worse time to impose DMA-style obligations. High-speed trains are not limited by their engines. It's the quality and trust in the tracks that hold them back. **The wrong kind of regulation will have small businesses moving at 20th-century speeds in a 21st-century race.**"

Background Execution Management

The DMA mandates that smart devices like your personal cellphone must provide full access to background execution—functions taking place out of sight, including when the phone is locked—to any developer of an app accompanying a third-party connected device like a smart watch, virtual reality headset, or other device made by a different company than your personal smart device. The DMA essentially forces personal smart devices like personal smartphones and tablets to allow other devices to leech off their built-in computing power. This creates a strong incentive for third-party developers to offload processing and background execution to the smart device, which would force slowdowns in other processes on the device. Users would see significant decreases in compute capacity for other apps, device overheating, battery drain, and other issues arising from forcing a smart device to accommodate more than it was designed to handle. Small app developers without their own devices would bear the brunt of this issue.

Mark Thomas, founder of UK-based Appnalysis: "Mobile operating systems are designed for a user-friendly experience. If you prohibit the operating system from managing the device's resources, you bring computing several steps backward to the pre-personal computer age**. The user experience will plummet, and I can't imagine that's what regulators have in mind.**"

Fee Structures

Right now, the two major consumer-facing app stores have progressive fee structures for companies distributing their apps on the store. The vast majority of apps and app developers, in non-DMA jurisdictions, pay no commission on revenue in exchange for developer services, including distribution of apps. For apps whose revenue stream depends on digital-only goods and services—such as skins for characters in videogames and unlocking messaging on dating apps—those charges are assessed a 15 percent commission on either Google Play or the Apple App Store. Both stores also charge app developers making more than $1 million in digital-only goods and services 30 percent on those digital-only sales, but these developers only account for a tiny fraction of all developers. Some of these multi-billion dollar companies are proponents of DMA because the law eliminates the distribution costs these companies bear now in non-DMA jurisdictions. Right now, the only DMA-compliant fee structure shifts the costs of maintaining and improving digital platforms downward to smaller developers like App Association members.

Sveatoslav Vizitiu, Romania-based founder of Rhuna: "Let's get something straight. Most of us don't pay any commission. My business is centered on improving the events and entertainment industry by tokenizing products, services, and experiences. That's not a digital-only service, so I don't pay a commission on sales. These companies complaining and agitating for DMA sell digital-only services and that's just not the majority of developers. Even most developers who pay a commission recognize they get value for the money. **Distribution isn't free, so I don't appreciate that the bigger companies are trying to shift more of those costs to my business through regulation.**"

Wi-Fi Mandates

The DMA would alter the current structure for sharing Wi-Fi passwords on Apple devices. As of now, iOS devices can share Wi-Fi passwords with nearby devices through a simple tap. This sharing is possible through the device-level storage of Wi-Fi passwords and other sensitive information, a structure which keeps the passwords secure. The DMA would require Apple to collect all the Wi-Fi passwords stored on your device and allow sharing with any other device, even those made by adversary countries who are known to steal such information. The goal of this provision in theory is to force Apple to not have a monopoly on this device feature, but in reality, it will open up your personal device to infiltration by nefarious actors, increasing privacy risks.

Mitchel Volkering, founder of Netherlands-based Vaic.at: "I provide services for job search candidates, who trust me and their smart devices with their personal information. If they go to an interview and their device connects to the Wi-Fi, DMA mandates that a third-party device has access to that information. After the interview, if the candidate is connected to that same Wi-Fi regularly, a third-party device now has that information too and can ascertain they must have gotten the job. **The fact that this information is now potentially for sale undermines my competitive position by giving all my competitors potential access to my client's information and also exposes my client to privacy risks associated with their Wi-Fi connection history.** Their movements can be tracked. It is not appropriate for government to create these problems. It certainly doesn't help my EU-based company, and it should serve as a warning for U.S. policymakers."