Insight

Europe's Digital Markets Act Has Global Implications

JEFFREY WESTLING | APRIL 19, 2022

Executive Summary

- In March, European legislators agreed to a framework for the Digital Markets Act (DMA) which would regulate "gatekeepers"—such as Amazon, Apple, Google, Meta, and Microsoft—in the digital economy to prevent them from engaging in practices that could produce anticompetitive harms.
- Business practices that produce anticompetitive harms in the digital marketplace could justify antitrust scrutiny, but the opaque process and goals of the DMA suggest that European regulators have dismissed concerns over this legislation in favor of simply targeting companies that, they argue, have grown too large.
- The DMA will have significant implications for the welfare of consumers as well as the cybersecurity of devices and services in Europe and across the globe.
- U.S. lawmakers should work with their European counterparts to address these concerns in the final text of the legislation and be wary of attempts in the United States to impose similar restrictions without a careful balancing of the costs and benefits.

Introduction

In March, European Union (EU) lawmakers agreed on a framework for the Digital Markets Act (DMA). In principle, the DMA would target "gatekeepers" of the digital economy—such as Amazon, Apple, Google, Meta, and Microsoft—forcing these companies to open their services to competitors and limiting their ability to favor their own products. European policymakers designed the DMA to promote competition in digital markets; nevertheless, these regulations may eliminate pro-consumer benefits that come with large firms, such as lower prices or strong cybersecurity in devices and services.

The practices that the DMA would likely target could produce some anticompetitive harms—such as a closed system limiting consumer choice in applications or an online store narrowing options to ensure the stores' own products outcompete rivals—and these harms could outweigh any benefits to consumers. Thus far, however, the opaque process and limited information with which the DMA has been crafted sheds little insight into whether European policymakers considered this balance at all. In early negotiations among the European Commission, the European Parliament, and EU member states, regulators proposed a wide range of regulations and restrictions that were shared generally with the public. Yet, with such a wide range of potential proposals on the table, interested parties struggled to determine which were serious and which would be cut during negotiations. Ideally, regulators would have made public the negotiations and debate so that interested parties could closely follow the developments, as the final text will drastically affect both companies and consumers across the globe. Instead, the discussions among the three entities took place behind closed doors. Now, interested parties must comb through reports and press releases to understand what the final text of the DMA will contain, though it will clearly target American firms (in doing so, harming Apple to the benefit of, say, Samsung, Xiaomi, and Huawei in the smartphone market) and set standards for practices such as interoperability and self-preferencing

of large firms.

While the Biden Administration has taken steps to work with Europe to address specific concerns with the legislation, the president has faced criticism from some in his own party, particularly Senator Elizabeth Warren, who argued that his administration was lobbying on behalf of Big Tech. Without any significant U.S. input over the development of the DMA, the regulation is likely to have a large, negative impact on American companies and consumers.

This insight breaks down the reported deal, explaining what the DMA will likely do and the impacts it may have on American businesses. Further, it attempts to demystify the "black box" that is the EU's approach to the regulation, as well as the protectionist principles underlying the regulation. Finally, the insight highlights the need for U.S. lawmakers to actively engage with their EU counterparts leading up to the likely final adoption of the DMA this summer.

The Digital Markets Act

While the details of the DMA haven't been formally finalized, the EU Parliament has stated that the regulations would target digital gatekeepers, defined as companies with a market capitalization of more than $83 billion and at least 45 million monthly users. In practice, this would cover the largest firms in the world, though it would primarily affect American tech companies. The DMA's classification of "gatekeeper" would come with a wide array of restrictions on the behaviors of covered companies, such as sharing data between the core platforms and other services, as well as self-preferencing of gatekeepers' own products over those of rivals or allowing sideloading onto app stores. The specific regulations would also include some requirements regarding interoperability, notably targeting messaging apps, including Facebook Messenger and WhatsApp, according to recent reports.

Of note, the DMA wouldn't necessarily replace existing antitrust tools, but would instead develop prohibitions to supplement current enforcement after harms have occurred. As the International Center for Law and Economics explains, the DMA "appears to blur the line between regulation and antitrust by mixing their respective features and goals." For example, the DMA would target specific practices "subject to past and ongoing antitrust investigations," filling perceived antitrust-enforcement gaps rather than addressing specific theories of harm. In other words, the DMA's preemptive regulation addresses perceived enforcement failures rather than market failures.

Despite the general awareness of what the legislation will include, the final details remain somewhat opaque. During the intake process, European regulators floated myriad ideas that could be included in the DMA. Negotiations are ongoing, however, and the talks among the European Commission, Parliament, and member states happened behind closed doors, meaning outside parties can only rely on press releases, statements, and reports to understand what may be in the final proposal.

Transparency and Protectionism: The Process Problems with the DMA

At the outset of the process, regulators conducted an intake that brought in a wide range of ideas to potentially include in the DMA. Most of this process was fairly transparent, with interested parties at least somewhat aware of a specific proposal's existence. Yet when determining what would make the final regulation, European regulators negotiated largely behind closed doors. Moreover, while consumer welfare and cybersecurity considerations should weigh heavily in these negotiations, reports indicate that regulators are instead focused on

filling perceived shortcomings of recent antitrust enforcement litigation—as well as specifically targeting American firms, potentially giving European companies a leg up on their American counterparts.

The Biden Administration has questioned some of the EU's decision-making, and worked with its European colleagues to address concerns about protectionism in the legislation. Specifically, the administration attempted to address concerns regarding how the DMA would harm cybersecurity practices, as well as technological innovation generally.

The administration has received pushback from some in Congress who embrace the "big is bad" approach to antitrust, however. After the Biden Administration shared its concerns publicly, Senator Warren sent a letter to the White House criticizing the comments, going so far as to claim the administration was lobbying on behalf of Big Tech companies.

Indeed, this type of anti-big tech sentiment has led to major antitrust legislation in the United States – most notably the American Innovation and Choice Online Act and the Open App Markets Act. Unfortunately, many of the same problems inherent in the DMA also exist in these bills, which also recently received support from the executive branch. Of particular concern, the bills would impose similar requirements that potentially undermine the cybersecurity of networks and devices, including forcing companies to weaken the security of their networks and devices to ensure that all rivals have access to consumers.

Impacts on Consumer Welfare and Cybersecurity

The American Action Forum's previous work on the DMA outlines the potential harms to consumers that could arise from this legislation. Increased market concentration can often come with beneficial integration and efficiencies, leading to innovative new products and services. For example, Amazon's Prime service and brands can offer lower prices and quicker delivery than rivals due to the integration of these products and services into the same model. With the DMA's restrictions on self-preferencing, this type of offering could be eliminated, meaning rival firms could have a better chance of competing but consumers may pay more for potentially worse-quality goods.

Even beyond the direct harm to consumers, the threat of cybersecurity vulnerabilities presents a potentially more significant concern. Forcing firms to open secure networks through interoperability requirements will undoubtedly come with challenges and risks to the cybersecurity of users. A messaging app interoperating with any rival app that seeks to connect with consumers inevitably makes it harder to crack down on spam messages and phishing attempts, and potentially could present challenges for encrypting communications. Requiring system operators to allow sideloading can lower fees and costs for app developers, but also opens the device up to malicious actors who can find new attack vectors on consumers, even those who don't sideload apps themselves.

Cybersecurity is only as strong as the weakest link and forcing companies to add more potential opportunities and incentives for malicious actors to attack will come with additional risks. The benefits to competition could outweigh the risks depending on how significant they are, but the DMA could abandon such analysis outright, or shift the burden to the gatekeepers to prove in court that the security risks outweigh the competitive harms.

As the EU considers such regulations, it should do so with a careful eye toward Russia, which has been engaging in more frequent and severe cyberattacks against Ukraine and many experts worry could extend to other western governments. As Margaritis Schinas, vice president of the EU Commission, explained at the Munich Security

Conference, “We cannot allow…malicious actors to penetrate our defenses, whether those of our institutions or those of our citizens’ daily lives.” Indeed, the White House voiced similar concerns, warning American firms to prepare for potential cyberattacks after Russia’s invasion of Ukraine.

With tensions escalating, cyberattacks on European and American citizens will undoubtedly continue to rise, and regulators on both sides of the Atlantic must recognize the need to remain vigilant. These targeted efforts to further regulate Big Tech will almost certainly increase the vulnerability of the internet ecosystem, and regulators should remain cognizant of this as they weigh the relative costs and benefits.

What Can U.S. Policymakers Do?

Even if U.S. lawmakers agree in principle with the goals of the DMA, they should actively engage with the EU to address concerns as specific language is drafted, especially insofar as U.S. cybersecurity efforts may be affected.

American policymakers should make clear to the EU the tradeoffs that come with restrictions on self-preferencing and transparency generally, as well as the harms to consumers and cybersecurity that could result from targeting American firms to protect European competitors. Again, perhaps even after careful consideration of potential costs and benefits, European regulators may determine the DMA is worth the tradeoffs. As it stands now, however, it appears these potential harms have been dismissed largely in favor of protectionism and a desire to regulate Big Tech.

While it may be too late for changes to the DMA, U.S. lawmakers must take care to avoid repeating the EU’s mistakes with their own legislation. A wide array of antitrust proposals has been introduced in Congress with similar bans on self-preferencing and requirements for interoperability. As Congress considers these bills, it should carefully weigh the potential tradeoffs regarding consumer welfare and cybersecurity, especially as the United States prepares for more cyberattacks from Russia and other international rivals.