SEPTEMBER 2021

# Implications of the Digital Markets Act for Transatlantic Cooperation

By Meredith Broadbent

## *Introduction*

On December 15, 2020, the European Commission introduced the **Digital Markets Act** (DMA). Proposed alongside the **Digital Services Act** (DSA), the package is targeted at reshaping business models in ways that would likely impede the market access of U.S. tech giants in Europe, namely Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) companies.

The DMA is a landmark proposal of *ex ante* competition policy that will add to the European Union's existing legal structure for competition regulation, which is based on evidence-based, case-by-case investigations. The DMA has two premises: that current competition policies have not delivered the desired result of reigning in the size, scale, and perceived dominant behavior of large U.S. online firms; and that disciplining the business practices of large U.S. tech platforms is necessary for Europe to improve its performance in the digital space. Many policymakers and the business community in the United States view the proposal as a direct attack on U.S. companies for being too big and too successful in Europe. The European Commission, on the other hand, appears convinced that the new *ex ante* regulation structure under the DMA will create opportunities for European tech companies to scale and become more globally competitive—a view the commission categorically declares but, in the author's view, is not likely to occur. A regulatory disabling of U.S. tech giants through the DMA could lead to perverse and unintended consequences for European businesses and consumers and for the strategic posture of Europe with respect to Chinese competition going forward.

As proposed, the DMA will amend the EU competition law system to the benefit of European incumbents and subsidized Chinese competitors. European officials have championed the DMA as a tool for achieving technological sovereignty in the European Union, and they have overtly identified successful U.S. tech

platforms as the intended targets of the DMA. Instead, these regulations should be scrutinized and then revised as necessary to ensure they do not function as discriminatory, unfair measures of industrial protectionism that could, if enacted, violate Europe's trade commitments at the World Trade Organization (WTO).

As the rapporteur assigned by the European Parliament to the DMA and the European People's Party coordinator in Brussels, Member of European Parliament (MEP) Andreas Schwab heads the development of the European Parliament's position on the proposed legislation. Schwab has repeatedly called for the need to limit the scope of the DMA to non-European firms. In May 2021, **Schwab said**, "Let's focus first on the biggest problems, on the biggest bottlenecks. Let's go down the line—one, two, three, four, five—and maybe six with Alibaba. But let's not start with number seven to include a European gatekeeper just to please [U.S. president Joe] Biden." The Schwab report, released in June, narrowed the initial scope of the DMA and increased the size thresholds, meaning the DMA would not apply to non-U.S. companies like the European-headquartered Booking.com. This discriminatory targeting of U.S. companies, in disregard of Europe's WTO obligations, raises questions about Europe's overall commitment to the rules of a multilateral trading system as they apply to tech platforms, digital services, and the digital economy.

A more balanced approach has been taken by Dita Charanzova, vice president of the European Parliament, who has urged a common transatlantic approach to digital regulation to counteract China, **saying**, "We must state the truth: these proposals [DMA and DSA] target U.S. companies. The businesses are both loved and hated, but not one can deny they are vital to the European economy."

## *Purpose of the DMA*

The declared purpose of the DMA is to **lay down** harmonized rules, ensuring "contestable and fair markets in the digital sector across the Union where gatekeepers are present." Since recent competition cases aimed at conduct have not delivered the desired market outcomes, the commission intends to intervene through a new regulatory structure to provide for *ex ante* discipline of gatekeepers in the digital sector specifically.

**Recital 3** of the DMA indicates that the law is not intended to address actual evidenced harm, but rather future harm that is being assumed or speculated:

> A small number of large providers of core platform services have emerged with considerable economic power. Typically, they feature an ability to connect many business users with many end users through their services which, in turn, allows them to leverage their advantages, such as their access to large amounts of data, from one area of their activity to new ones. . . . As a result, the likelihood increases that the underlying markets do not function well—or will soon fail to function well.

Digital business models—such as large online tech firms, social media networks, e-commerce shopping sites, and video platforms—enable individuals and businesses all over the world to interact, trade, and conduct transactions with one another in innovative and more efficient ways. The DMA argues that these tech companies have become winner-take-all businesses and criticizes the advantages created through burgeoning networks effects that attract more and more users to the platforms. Both the United States and Europe are debating the merits of proposed revisions to antitrust law to address concerns brought about by the large market power and capitalization of U.S. tech champions. Europe is farther down the road in this debate but has yet to demonstrate that the new revolution in competition law and policy proposed in the DMA will not further suppress innovation and entrepreneurship in Europe.

## *Contents of the DMA*

**GATEKEEPERS**

As currently proposed, the DMA affects the following eight categories of core platform services:

(1) social media networks, (2) search engines, (3) video platforms, (4) communication services, (5) intermediation services, (6) cloud computing services, (7) operating systems, and (8) advertising networks that operate alongside any of the above.

The companies that will be subject to these DMA regulations are what the European Commission refers to as "gatekeepers." These gatekeepers are entities that have an outsize influence on the European Union's internal market, have functional control as a "gateway" for companies to reach end users and consumers, and have maintained their size in the European Union's internal market for three years. Specifically, gatekeepers are entities that fulfill the following criteria: (1) 45 million monthly users (equal to roughly 10 percent of the EU population), (2) global turnover of or exceeding $7.9 billion (€6.5 billion), and (3) operations in at least 3 of the 27 EU member states.

While these thresholds are meant to provide guidelines for a working definition of "gatekeeper," the commission nevertheless reserves the right to investigate companies that do not meet the formal definition of a gatekeeper. In other words, the DMA provides the European Commission with significant leeway to undertake investigations, creating additional uncertainty for firms as to whether or not they will be investigated and for which specific services they provide.

## *Article 5*

Article 5 of the DMA is the core chapter, along with Article 6, that lays out rules for gatekeepers and their obligations to end users and third parties. Article 5 consists of seven obligations that together constitute the most fundamental pillars of the DMA. Article 5(a) prevents the combination of personal data from other services offered by the same platform. For example, this could prevent Facebook from harvesting personal data from Instagram, and exporting that same data to Facebook, where it could target new advertising to that user based on the same data. Article 5(b) prohibits gatekeepers from providing services at different costs and conditions across various platforms via third-party intermediaries, and it builds in protections to allow businesses to interact with consumers outside of the core platform service. The fourth obligation established under Article 5 prevents gatekeepers from restricting the ability of business owners to raise "issues with any relevant public authority." Article 5(e) stipulates that gatekeepers must "refrain from requiring business users to use, offer, or interoperate with an identification service of the gatekeeper." Article 5(f) precludes the ability of gatekeepers to force businesses or end users to subscribe to the core platform service as a condition of accessing those services. The seventh and final obligation of Article 5(g) establishes transparency guidelines in advertising prices, stipulating that advertisers and publishers reserve the right to request data on ad relevance and revenue. This stipulation has led to industry concerns that third parties will be able to free ride on the proprietary capabilities of larger platforms that have been foundational to their innovative successes.

## *Article 6*

Article 6 primarily deals with **self-preferencing**, discriminatory ranking, and data-sharing obligations not dissimilar to those outlined in Article 5(g). For example, if a consumer was searching for a digital assistant

on Amazon, Amazon would be prevented from providing Alexa with favorable or even different treatment vis-à-vis Google Home or another competitor. Article 6(1)(a) prohibits the use of non-public data by gatekeepers. This rule affects gatekeepers' ability to gather data generated by both end users and business users. Another rule in Article 6 mandates that end users must be able to uninstall pre-installed applications. For example, this would preclude a scenario in which Apple prevents iPhone users from uninstalling the Apple App Store and using a third-party app store to make app purchases. Furthermore, as currently written, the DMA's language lacks a clear distinction between what constitutes an application or operating system. Failure to adequately distinguish between the two could potentially come at significant cost to companies maintaining operating systems, which, if required to make components of their operating systems distinct, could be forced into making fundamental—and very costly—design changes on both the back and front ends of products.

Article 6 of the DMA also prohibits self-preferencing, particularly by search engines. Furthermore, it mandates nondiscriminatory ranking for third-party providers of online search engines, and it establishes guardrails to prevent discrimination within application software stores. On a more granular level, Article 6 stipulates that gatekeepers must ensure interoperability between third-party software applications. While Article 6(1)(c) specifies interoperability parameters, the section does not include specific language that would protect trade secrets. It does, however, leave room for gatekeepers to ensure that third parties are not harming the gatekeeper's underlying software or hardware. Article 6(1)(f) addresses interoperability in a highly ambiguous way, stating that gatekeepers must "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware, or software features that are available or used in the provision by the gatekeeper of any ancillary services." While this language does not go so far as to mandate an open-source business model, it nevertheless poses serious questions about the degree to which companies designated as a gatekeeper would be forced to share trade secrets or design their technology in a way that directly advantages their competitors and limits their ability to differentiate their own products and service in competition with rivals.

Article 6(1)(h) creates rules for gatekeepers to facilitate data portability in order to prevent siloed storage of user data that would otherwise lead to users to be locked into certain platforms. Article 6 also mandates gatekeepers to provide advertisers, and publishers access to "performance measuring tools," which, in compliance with the General Data Protection Regulation (GDPR), may include data on ad revenue. This type of data effectively constitutes the "secret sauce" at the very core of several gatekeepers' business models. Article 6(1)(i) specifies that gatekeepers must provide business users and authorized third parties with "high-quality, continuous, and real-time access and use of aggregated or non-aggregated data." Overall, the obligations laid out in Article 6 of the DMA cover a wide range of practices that are typically used by platform operators to address what they see as market failures on their platforms, negative network effects, and governance issues. With these prohibitions in place, designated gatekeepers' services will be less flexible and able to evolve over time to meet changing market conditions and new challenges.

In addition to laying out a new regulatory framework for large technology firms, the DMA also contains language for suspensions, exemptions, market investigations, and enforcement. The DMA requires the European Commission to designate gatekeepers within six months of conducting an investigation. Fines for failure to comply reach as high as 10 percent of a company's global turnover. Unlike the DSA announced on the same day, DMA compliance and enforcement competencies are placed both with the European Commission and with member states' domestic antitrust enforcement measures.

The DMA, in its current form, would grant new regulatory authority to Brussels on gatekeeper regulation and enforcement. However, national competition authorities, as well as private entities, would also gain

enforcement power based on the DMA. This would be in addition to the option of taking more traditional antitrust and enforcement measures against gatekeepers in national courts and regulatory bodies. This contrasts with the DSA, where domestic regulators will have a responsibility to define and address sensitive freedom of speech topics, such as disinformation and hate speech.

## *Comparison of the DMA to Current Antitrust Approaches*

Traditional antitrust law, administered and enforced in the United States through courts, the Justice Department, the Federal Trade Commission, and state attorneys general, permits market leadership and large firms. Even potentially harmful conduct is permitted as long as it creates, on balance, improved efficiencies and benefits for consumers, including lower prices. In fact, competition enforcement in most developed markets around the world has trended toward an objective, economic, effects-based approach focused on establishing anticompetitive conduct through due process. These investigations put weight on efficiency objectives and consumer welfare, rather than targeting a certain level of market concentration. On the other hand, as CSIS has previously **observed**, antitrust enforcement officials in Europe "have tended to favor protecting potential competitors, even if market leaders have managed to outperform competitors and gain consumer loyalty through their ingenuity and smart acquisitions."

> *As a sweeping overhaul of European competition policy, the DMA could threaten certain operations of U.S. firms in Europe, discriminate in favor of European companies, and provide opportunities for systemic rivals—namely China—to achieve long-term geopolitical gains.*

The DMA, on the other hand, constitutes a dramatic turn to the use of an *ex ante* regulatory mechanism intended to overlap and operate in parallel with traditional European antitrust methods. As a sweeping overhaul of European competition policy, the DMA could threaten certain operations of U.S. firms in Europe, discriminate in favor of European companies, and provide opportunities for systemic rivals—namely China—to achieve long-term geopolitical gains.

## *Driving Forces behind the DMA*

European Commission officials, MEPs, and constituents have been impatient with evidentiary burdens, due process requirements, and the slower method of establishing anticompetitive behavior in the context of current European law and regulation. With growing control over platform ecosystems, gatekeepers are viewed as an anticompetitive threat because of their size, access to data, and corresponding ability to leverage their know-how and dynamic capabilities—including data collection and processing—to improve, develop, or offer new services in adjacent markets. European officials see the opacity, complexity, and size of gatekeeper ecosystems as thwarting the European Commission's ability to achieve desired outcomes in traditional antitrust cases.

Illustrating this point, the commission **states**:

> The Digital Markets Act addresses unfair practices by gatekeepers that either (i) fall outside the existing EU competition control rules, or (ii) cannot always be effectively tackled by these rules because of the systemic nature of some behaviours, as well as the ex post

> and case-by-case nature of competition law. The Digital Markets Act will thus minimise the harmful structural effects of these unfair practices ex ante, without limiting the EU's ability to intervene ex post via the enforcement of existing EU competition rules.

Margrethe Vestager, executive vice president of the European Commission, echoes the intent in a December 2020 **public statement**:

> And as you know from the cases that the Commission has been doing, where I have been responsible for, is not in one, not in two but in three Google cases, and also in the first Amazon case concerning e-books we have seen this behaviour. Many national authorities have also dealt with the issues caused by digital platforms as in the Booking.com cases. Complaints keep coming through our doors and those of fellow national enforcers, leading to a number of ongoing competition investigations. . . . antitrust will have to work hand in hand with regulation. So that we have a complete set of tools.

The European Commission **argues** that the existing regulatory environment will result in "a few large online platforms" that would determine "the parameters for future innovations, consumer choice, and competition," while preventing small European online platforms from scaling. The commission bases its views on the assumption that innovation will come only if new entrants and smaller companies have the purview to challenge large U.S. online platforms. Through the DMA, the commission claims that it seeks to create a fair-trading environment and increase innovative potential in online platform ecosystems in the European Union's single market. The commission **claims** that the DMA is "not Competition Law 2.0," but rather is inspired by the lessons that the commission has **learned** from the challenges of competition enforcement of digital companies in the last 15–20 years.

To stakeholders, it seems clear that the prohibitions of certain conduct under the DMA and the imposition of proactive obligations would only apply to major U.S. platforms, not their European or Chinese competitors offering similar services.

Shifting the focus of competition intervention from efficiency to market-structure objectives would push competition law in a new direction toward a structural ("big is bad") approach that favors smaller European competitors. U.S. platforms are particularly concerned with the prohibitions and obligations that would limit their ability to engage in conduct that is pro-competitive, efficient, and welfare-enhancing. In other words, a company's size will determine whether the new set of *ex ante* competition rules apply to it.

That approach would ignore the dynamic competition that gatekeepers bring to the market, the consumer welfare generated by the existing framework, and the innovation and investment incentives necessary to generate future technological breakthroughs.

The European Commission's Regulatory Scrutiny Board, tasked with reviewing the commission's justification for the new regulation, expressed concern with the lack of evidence supporting the underlying assumption of the DMA with respect to whether there are clear negative outcomes of gatekeeper behavior. The board went on to **urge** the commission to "consider the negative consequences of curtailing size advantages following from network economies and economies of scale for consumers."

## *The Decline of Europe's Digital Services and Technology Sector*

Looking at the issue historically, *The Economist* magazine recently **pronounced** a "decline of corporate Europe that is truly striking," particularly in the technology and digital services sector. With a mar-

ket of over 450 million consumers, a sophisticated workforce, an advanced education system, and a cutting-edge research and engineering base, Europe has failed to nurture indigenous digital platforms of significant size.

*The Economist* characterizes "the absence of European tech giants" as symptomatic of an ''entrepreneurial deficiency" that is in part caused by the relative difficulty in raising capital from private investors for start-ups in Europe. The United States, by contrast, has generated trillion-dollar valuations for software and e-commerce businesses that are upending the global economy.

Europe is home to only three technology companies (both hardware and software) in the **Fortune Global 500**, compared to twelve from the United States, six from China, six from Taiwan, and eight from Japan. Although Europe experienced **increased** technology investment in 2020, it still lags behind the United States and Asia. In 2020, European technology companies received $41 billion in capital investment, compared to $74 billion invested in Asian technology companies and $141 billion invested in U.S. technology companies.

Europe's overall decline in innovative digital services can be characterized by **several trends**:

1) European start-ups have struggled to scale up into major companies, especially in the digital and health sectors. Europe's success in turning start-ups into "unicorns" (private start-ups valued at $1 billion or more) is about half that of the United States, as investors and their capital are relatively scarce.

2) Europe is attracting a declining share of global research and development (R&D), particularly in the digital sector. R&D spending in 2018 by European software and computer firms was roughly 8 percent of the global total, **compared** to 11 percent for Chinese companies and 77 percent for U.S. companies.

3) As digital technologies become a driver of performance for global firms in all sectors, Europe has become less central to international digital trade flows due to the virtual absence of European companies in the digital platform space. Only **two-thirds** of digital potential was reached by European firms compared to their U.S. counterparts. In other words, European firms are far less digitized overall than U.S. firms. **Only 21 percent** of European firms have broadly adopted cloud services (versus 33 percent in North America). Failure to embrace cloud infrastructure (which right now is only really offered in Europe by U.S. firms and Alibaba) appears to be suppressing sectoral and national digitization efforts. The slow adoption of cloud services by European companies has been loosely attributed to concerns over interoperability, portability, and data control challenges.

A hopeful sign is that European start-ups have proven to be more efficient than U.S. start-ups in their use of venture capital funding, possibly due in part to the relative shortage of venture capital in Europe. According to Pitchbook, a data provider, it takes **50–100 percent** more capital funding in the United States than in Europe to start a company that reaches unicorn status. European start-ups reach unicorn status with much lower totals of venture capital than U.S. rivals. Nevertheless, PitchBook cites statistics that in the last decade, while venture capitalists globally have backed 661 unicorn companies total, only **78** of them have been in Europe.

Given these challenges, it would be wise for Europe to tread slowly in adopting new regulatory policies that risk further suppressing the climate for innovation in Europe.

## *Distinguishing Digital Markets from Non-digital*

An underlying premise of the DMA is that digital markets can be separated from non-digital markets for purposes of applying *ex ante* regulatory requirements. The DMA defines the digital sector as "the sector of

products and services provided by means of or through information society services." In fact, as the Information Technology and Innovation Foundation observes in a recent **paper**, "the digital sector cannot be easily distinguished from the non-digital sector."

> *With increasing technological innovation, digital now applies to many sectors of the economy, including banking, entertainment, real estate, etc. It is unclear under the draft DMA proposal what ratio of physical versus digital sales is necessary for a company to be considered a digital company.*

A digital channel is one of many ways that firms reach consumers, often simultaneously, and the various mechanisms have become increasingly intertwined. To distinguish between digital and non-digital companies, it may be necessary to recognize that digital is essentially a business model and distribution mechanism, rather than a market. Competition, however, takes place in the product market, not in any particular distribution channel. With increasing technological innovation, digital now applies to many sectors of the economy, including banking, entertainment, real estate, etc. It is unclear under the draft DMA proposal what ratio of physical versus digital sales is necessary for a company to be considered a digital company.

## *Stakeholder Views on the DMA Proposal*

Pro-innovation EU member states have expressed concerns in the press about the suppressing effects of hard regulation under the DMA on future innovation in the European Union. A representative of Estonia, for example, **warned** that "it is crucial to refrain from over-regulating online service providers" and urged the European Parliament and European Council to "carefully weigh every measure's impact on consumer welfare, innovation, and business users' legitimate interests." Claiming that "practical applicability" is key, a representative of Latvia **urged** a "proportionate and evidence-based approach" and "compatibility with the existing EU competition legislation, the Digital Services Act, and platforms to business regulation."

In all, the European Commission **received** 90 stakeholder comments, 41 percent of which were submitted by business associations, 25 percent by companies, and 16 percent by nongovernmental organizations. Research institutions, private consumer groups, trade unions, and private citizens also filed views. The majority of the comments were submitted by stakeholders based in Belgium, Germany, and France—60 percent collectively. Views expressed tended to center on the following themes: (1) the need for more precise definitions and criteria for gatekeepers, business users, and end users; (2) concerns about the division of authority between national authorities and the commission; (3) the desire for specification of core platform services; and (4) questions about what should or should not fall under the scope of the DMA.

Multiple comments requested greater clarification about how exactly gatekeeper status would be assessed. Several groups, including Allied for Startups, Santander Bank, and AdDigital (Spain's digital association), pointed out that the qualitative and quantitative thresholds established in the DMA could discourage growth of new businesses and possibly deter EU digitalization. On the other hand, the European DIGITAL SME Alliance, a business network group that promotes technological sovereignty for Europe, is supportive of self-preferencing restrictions on gatekeepers, the right of users to install third-party software, and obligations to provide access to online advertising tools.

Additionally, multiple concerns were expressed about how business users and end users are defined. As Booking.com made clear, the end user of Facebook often is not the same as an end user shopping on a merchant site. In the context of Facebook, a user could access facebook.com without logging in and thus would not be engaging with the service in the same way that someone logged in would. In the context of shopping sites, is an end user someone who makes a purchase or someone who visits and browses the sites, thus generating data for the site? Airbnb notes that this clarification is needed, otherwise obligations cannot be tailored to the gatekeeper's business.

The DMA does not clearly define or accommodate these nuances. Other commenters pointed out that the DMA does not consider how these definitions might evolve in the future, based on evolutions in the market or how a gatekeeper's status could change after being initially determined. Eco—Association of the Internet Industry called for better standards on how gatekeepers would be designated in the future. EMISA, a business association, noted the need for a complaint mechanism where market players (competitors)—not just member states—can submit complaints.

The DMA also establishes a list of core platform service types that generated considerable stakeholder feedback. Groups like the European Publishers Council and News Media Europe call for the specific inclusion of web browsers into the list of core platform services. There are also calls to eliminate certain services from consideration. Microsoft and IBM urge the exclusion of Infrastructure as a Service (IaaS) and cloud computing providers from consideration. Microsoft points out that cloud services act as more of an input and do not intermediate the business relationship between end users and business users in the same way that other core platform services, like online shopping platforms, do.

Finally, multiple comments cited confusion about the division between national authorities and the European Commission. The German Federal Bar association notes that the DMA does not specify the distinction between national law, competition law, and fair-trading law, and that the rules of enforcement are not clear. As DuckDuckGo points out, it is not clear if national authorities will play a role in enforcement, though the company argues they should. Several member states have called for more clarity with respect to coordination between the DMA and the GDPR, the Regulation on Platform to Business Trading Practices, and legislation related to the protection of intellectual property rights.

Comments obviously varied, often based on the implications that the DMA would have on the businesses submitting the comments. Some member states have called for adjustments to proposed obligations concerning interoperability, data portability, and access to data. There is a general sentiment for more clarity and precision with respect to many definitions and obligations under the DMA.

Some member states have **proposed** "a possibility of gatekeepers to make use of efficiency and objective justifications for their conduct to better take into account the impact of gatekeepers' behaviour on consumers and the particular situation of each gatekeeper." In a strong division of views on adding a possible appeals process for being designated for controls under the DMA, "other Member States were of the opinion that such a possibility would weaken the DMA and make its enforcement more cumbersome, lengthier, and less effective."

Several recent economic studies have raised serious concerns about the negative, unintended results the DMA could have on suppressing innovation in Europe. Oxera **claims**, "the Digital Markets Act needs more consideration as it is likely to reduce the benefits of innovation for European consumers and businesses." Compass Lexecon **finds** that "the proposal lacks procedural safeguards as well as a feedback mechanism for the EC to adjust it. Without these safeguards, the benefits of *ex-ante* obligations do not outweigh their

costs." **Copenhagen Economics claims** that "EU firms may face reduced productivity and competitiveness as the proposed DMA may impair some of the functionalities of digital platform services that create value for the users."

The DMA could slow the adoption of digital technologies by European industry for three main reasons:

1) Increasing regulatory costs will drive up barriers to entry, thereby reinforcing rigidity in the economy and status quo companies. Incentives for smaller and medium-sized platforms to innovate and scale up will be suppressed, as anticipated threshold effects inject uncertainty into their calculations; growth and success will be met with increased regulatory scrutiny, possible legal liability, and an anticipated inability to claim the earned monetary rewards of their innovative efforts in Europe.

2) Analysts express concern that the DMA's *ex ante* regulatory proposals will reduce incentives for large online platforms to provide new, innovative products and services to European businesses and consumers. Restrictions on gatekeepers, including prohibitions on bundling and adjacent market entry, would directly suppress the ability of platforms to innovate by developing new products and services for customers. Specifically, Articles 5 and 6 overlook the innovation dynamics resulting from the initial creation and subsequent innovations of a service. Companies who are closing in on the threshold for meeting gatekeeper status may be disincentivized from creating a new service that would bring in additional users. For example, this concern could persuade a large platform provider against investing in a new telehealth channel with on-demand services for fear of outgrowing its established regulatory category. DMA restrictions will hamper existing gatekeepers from competitively constraining one another, particularly outside of their own "lane," for example, Apple with search or Microsoft with digital advertising.

3) As large online platforms are constrained, opportunities for natural affiliations between relatively less digitized European firms and highly digitized U.S. firms will be reduced. In the author's view, maintaining and enhancing a competitive global advantage will require European firms to leverage relationships with U.S. tech firms to speed up digitization efforts. As an example, pressure to digitize is particularly acute in the world-class German automobile sector. Companies like BMW and Volkswagen are pivoting, like the rest of the global industry, toward the production of autonomous vehicles, which produce on the order of **1GB of data** each second. Unable to store and process this data on their own, German automobile manufacturers have partnered with U.S. cloud service providers, including Microsoft, to advance their digitization efforts. Further underscoring this objective to digitize, the Verband der Automobilindustrie, Germany's major automotive association, **made public** an industry effort to invest €40 billion ($47.1 billion) in e-mobility and €18 billion ($21.2 billion) in digitization between 2019 and 2021. In addition, in June 2019, Volkswagen **announced** it would spend €4 billion ($4.7 billion) on digitalization.

As consumer interests become more sophisticated and the deployment of goods like autonomous electric vehicles accelerates, analog companies will be less able to meet market demands. Maintaining strong commercial ties across the Atlantic therefore benefits U.S. and European firms alike. However, in the case of autonomous vehicles, it is the sheer size of U.S. firms, particularly cloud operating firms, that enables them to support sophisticated European manufacturers seeking to digitize. These virtuous partnerships should be embraced by European and U.S. government officials for their positive impact on supporting innovation in new areas of technological challenge, such as harnessing technology (including artificial intelligence [AI]) to support smart cities, in ways that will uphold Western values of privacy and human rights.

In contrast to a willing exchange of technology within the negotiated legal framework of commercial partnerships, the DMA's regulatory obligations to share data, grant access, and turn over proprietary innovations will

allow competing firms to copy market leaders' innovations. Government mandates to share data with competing firms can be expected to have a chilling effect on resources devoted to advancements in data analytics, because gatekeepers will be required to make this knowledge available to competing firms for free.

## *The DMA's Impact on the Protection of Intellectual Property Rights*

In their recent **communiqué**, G7 nations pledged to strengthen "rules to protect against unfair practices, such as forced technology transfer [and] intellectual property theft," used "to gain competitive advantage." This promise could be threatened if the DMA were to become law as proposed without further clarification.

Forcing U.S. companies into disclosing proprietary intellectual property, including sensitive trade secrets, proprietary data, and prized source code for algorithms, would be an unwise measure that will unfairly benefit European as well as Chinese and Russian competitors.

In addition, these requirements call into question basic national treatment and nondiscrimination obligations that are central to the WTO Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement. The DMA requires gatekeepers to disclose proprietary information, user data, internal tools, details of technical infrastructure, and other intellectual property to competitors. The DMA also forces gatekeepers to provide competitors access to key system hardware and software features and to provide continuous, real-time access to data generated on their platforms. In addition, the DMA calls on gatekeepers that supply search engine services to disclose to their competitors how they rank answers to a given query. This requirement would force U.S. companies to disclose sensitive trade secrets and expertise while their EU competitors are not subject to the same requirement. Additional requirements compel gatekeepers to disclose information on interoperability and performance-measuring tools.

*Forcing U.S. companies into disclosing proprietary intellectual property, including sensitive trade secrets, proprietary data, and prized source code for algorithms, would be an unwise measure that will unfairly benefit European as well as Chinese and Russian competitors.*

Imposing such requirements on U.S. companies and not on their EU counterparts, without an effects-based assessment into the proportionality or necessity of these requirements that afford the defendants due process and rights of defense, likely violates the national treatment obligation in Article 3 of the TRIPS Agreement, as well as the substantive provisions of Article 39 of the TRIPS Agreement regarding the protection of undisclosed information.

## *Value of Platforms to Consumers and Business Users*

Frustration on both sides of the Atlantic with the incredible size of large platforms should not give regulators and politicians license to disregard the value being provided to consumers and business users through the stimulation of innovation, growth, and employment. Large tech companies develop and provide services for thousands of companies and millions of consumers worldwide. Value creation is delivered primarily through intermediation, aggregation, and dynamic competition. Intermediation can range from a relatively simple interaction, such as a platform facilitating messaging between two people, to a platform like Facebook hosting a live fundraiser that is broadcast to millions of people around the world, providing a not-for-profit initiative with a free platform and large audience.

Secondly, platforms create **value** by aggregating data. Aggregation can assume several forms, including allocative efficiency (increasing market competition and helping consumers find the right products quickly), product efficiencies (enabling economies of scale, which lowers consumer prices), and transaction cost reduction (creating a trustworthy environment that mitigates transaction friction). In the case of data aggregation companies, consumers might agree they benefit when firms like Amazon target consumers with more appropriate ads based on past purchase and browsing history, while reducing the cost of goods and necessary browsing time for consumers. On the other hand, many consumers see this service as a misuse of their personal data.

Large platforms can create dynamic competition by providing a relatively certain, trustworthy environment, allowing developers and small businesses to leverage existing features to create unique products and add-ons that increase competition and innovation. Importantly, platforms create substantial value in the maintenance of both physical infrastructure (such as servers and undersea cables) and policy infrastructure (such as community and product standards). Whether aggregating data to reduce inefficiency or providing frameworks to enhance dynamic competition, platforms add significant value to consumers and businesses alike, in spite of, or perhaps due to, their size.

## *DMA Restrictions on App Stores and App Development*

Both the United States and Europe are wrestling with concerns about market power being exercised by Apple's App Store and Google's Play Store in the form of high prices and controls over their respective digital ecosystems. In the United States, court cases against **Apple's App Store** and **Google's Play Store** address similar competition and pricing issues that the DMA seeks to discipline in Europe.

Epic Games, the developer of the popular gaming app Fortnite, sued Apple, stating that since iOS users can only access apps through the Apple-owned App Store, Apple has too much control over app distribution. Apple, on the other hand, argues that it does not have a monopoly over app distribution since it shares the market with Google's Android platform and users are also able to play the game on other platforms like gaming consoles.

Several state attorneys general in the United States have **filed** a lawsuit against Google, alleging that it is unfair for companies to be required to pay Google's 30 percent commission on their annual app store revenue. The company **argues**, however, that Android allows users to access multiple app stores, providing app developers several avenues to reach Android users. Thus, if app developers wish to avoid the Play Store's terms and conditions, they will still have access to the Android platform. Although both the Apple and Google lawsuits remain undecided, the verdicts could result in increased regulatory scrutiny in the United States that may be in line with some of the DMA's proposed measures.

Under the DMA proposal, Apple and Google would be subject to new obligations aimed at enhancing the position of the platforms' business users. For example, under the DMA, limitations could be imposed on the size of commissions Apple and Google can charge on transactions concluded via their app stores. The European Commission is concerned that Apple does not permit its competitors to inform users about the possibility of buying their products on platforms other than the App Store, perhaps at a cheaper price. Apple and Google would also be required to facilitate "sideloading," in which users bypass the Apple and Google app stores, including accompanying security protections, in order to install apps directly on their phone from third-party stores.

Several business issues arise from the DMA requirement that Apple and Google **permit** "sideloading." First, a proliferation of app stores—a potential direct result of Article 6(1)(c)—will ultimately increase the costs for app

developers, especially small and medium-sized enterprises (SMEs). For a developer, making an app available across several app stores requires a significant investment, and the process is especially burdensome for SMEs.

Currently, Apple and Google run their platforms on different programming languages and have different interfaces and interaction flows. Thus, a developer designing an app available on two app stores must invest in two different types of technical knowledge. With an influx of stores available, developers must decide which ones to use to release their products. These decisions affect app design, programming interface, and additional characteristics, all representing additional costs.

Future app stores may not have the same trust and consumer safety standards currently present in the Apple App Store and Google Play Store. For example, known developers must abide by Apple's guidelines. Apple has a **team of 500 technical experts** who review an average of 100,000 new apps each week. Apple's size in part enables it to dedicate these types of resources to building a secure environment. Because of risks inherent to the internet, such as downloading malware, consumers generally favor apps from well-recognized, larger developers at the expense of apps from lesser-known, smaller developers. Well-known app stores are generally preferred by app developers because of the broad exposure offered to potential customers. Onerous DMA regulations could constrain future investments Apple and Google choose to make in upgrading their app stores by developing better services for developers. Scaling back services offered to developers, including advertising tools and payment services—which SMEs do not have the resources to manage and develop on their own—could raise costs and market access barriers for small developers.

For app developers seeking to monetize their hard work and innovation, the large size of online platforms offers value for its ability to draw consumers. The more traffic the app store can attract, the more consumers will benefit from a higher quantity and quality of apps. Consequently, large app stores such as Apple's App Store and Google's Play Store can be advantageous for small app developers, as developers can utilize the app store's broad user base to reach consumers across the world, a scale of exposure that was unimaginable for an SME in the past.

The DMA also raises legal uncertainty, which may hurt innovation and small developers. As currently written, the DMA provides the European Commission with the authority to undertake a periodic review of gatekeeper designations and update the threshold criteria as it sees fit. As a result, a threshold that is constantly shifting may discourage larger platforms from scaling up, further entrenching current gatekeepers and slowing innovation. Nevertheless, if the list of gatekeepers does continuously expand, SMEs—including small app developers—will face the most severe consequences, as these firms have fewer internal resources for adapting to changing market conditions brought about by evolving designations of gatekeepers.

Indicative of an emerging division of industry opinion surrounding the DMA, some of Apple's and Google's key competitors, such as Spotify and Epic Games, have banded together to form the **Coalition for App Fairness**. The coalition coordinates industry and developer efforts to demand **fairer practices** from Apple and Google, including changes to specific policies, such as lack of competitive options for iOS, self-preferencing of Apple's and Google's own products, and the charge of up to 30 percent annually for digital subscriptions sold through app stores. Given costs and damage to public image stemming from a myriad of high-profile legal battles, it is possible that a transatlantic set of best practices could be hammered out between U.S. and EU regulatory officials, app stores, developers, and other business users. The guidelines could address some of the large platforms' most controversial practices, while preserving the benefits of wide reach and data security that small app developers enjoy on these two large platform stores.

## *Cloud Computing, Data Sharing, and Security Concerns*

In 2018, the following cloud computing firms **held** these market shares for IaaS Public Cloud Services in

Europe. The cloud computing market in Europe is evolving quickly, and annual growth rates, particularly of the smaller players, are resulting in fast-changing market shares.

- Amazon – 47.8%
- Microsoft – 15.5%
- Alibaba – 7.7.%
- Google – 4.0%
- IBM – 1.8%

Market share growth rates in 2018 were:

- Alibaba – 92.6%
- Microsoft – 60.9%
- Google – 60.2%
- Amazon – 26.8%
- IBM – 24.7%
- Others – 11.1%

The DMA broadly includes cloud computing in its definition of core platform services. Any core platform service, including a cloud computing service, that meets the gatekeeper thresholds established by the DMA will be subject to the obligations in **Articles 5 and 6**. Notably, Article 6(1)(i) would require that gatekeepers "provide business users or third parties authorized by a business user, free of charge, with effective, high-quality, continuous, and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products or services."

Based on the DMA definition of cloud computing, major cloud computing service providers Amazon Web Services (AWS) and Microsoft Azure would be included in the scope of the DMA and would meet the established gatekeeper thresholds. The contextual issue of cloud computing raises several questions about the DMA's definition of "business user" and "end user." For example, who qualifies as a business user of AWS? Is Netflix, which uses AWS to host its website and acts as a commercial service seller, an end user? Alternatively, do cloud computing services, particularly IaaS providers, not have business users in the sense of the DMA? Would Netflix be an end user in this example?

*The DMA broadly includes cloud computing in its definition of core platform services. Any core platform service, including a cloud computing service, that meets the gatekeeper thresholds established by the DMA will be subject to the obligations in* ***Articles 5 and 6.***

Currently IaaS is included within the scope of the DMA. If IaaS firms are determined to have business users under the DMA, then cloud computing services would be obligated to share user data with business us-

ers under Article 6(1)(i). Given the use of cloud computing in national security and critical infrastructure, this poses obvious security risks. Microsoft has argued in their comments on the DMA that IaaS should be excluded from the DMA's definition of cloud computing services because IaaS providers do not "intermediate" the relationship between business users and end users in the same way that an online marketplace like Google Shopping does.

The **Organization for Economic Cooperation and Development** has identified several risks associated with data sharing. Granting access to and sharing data may expose certain parts of the information systems to digital security threats. Personal data breaches (such as a leak of user data of employees at a government agency) are more likely to occur at points where data is accessed and shared. Evidence has indicated that data breaches increase with the collection, processing, and sharing of large volumes of data, and a high level of data agglomeration would be needed to comply with the DMA's data-sharing requirements.

There is a high likelihood that data sharing could run into issues with confidentiality agreements and contractual terms with data users, such as government agencies. Additionally, there are risks with the actual data that is being shared, such as employees' personal information.

Disclosure under the DMA would make an entity's business user data set publicly available, according to a **European Commission-sponsored report** from a group of economists. This public information would include details about which agencies and critical infrastructure groups are using which cloud computing services and how they are employing the services, possibly exposing weaknesses for ransomware attacks and other cybercrimes. Given that the European Commission itself uses Microsoft Azure and AWS, it is likely that the European Union has considered security risks. The European Commission may view GDPR requirements as sufficient for mitigating risk, but even so, this is a proposition that must be studied closely. Additionally, the commission has **committed** to an initiative on the creation of a shared European cloud, which would certainly impact an assessment of future vulnerabilities.

Alibaba, a Chinese company, has been making efforts **to expand its global footprint**. Currently, Alibaba would not hit the threshold needed to be considered a gatekeeper under the DMA. However, market access restrictions imposed under the DMA against the two U.S. cloud firms would likely **give** Alibaba a growth opportunity. This is particularly concerning in light of the Chinese government's plan to oversee data collected by its tech giants.

## *Considerations with Respect to Enhancing China's Access to the European Market*

Recognizing the "growing challenge posed by China and its discriminatory, authoritarian, and non-market approach to the digital realm," U.S. legislators, on a bipartisan basis, are **urging** "joint [U.S.-EU] approaches based on shared values" to digital platform regulation. One of the toughest areas of confrontation between the West and China is, in fact, in the digital space, where Chinese authoritarian practices, state subsidies, and a highly closed market have created friction and confrontation between Western countries and China. Although it is hoped that China will eventually open its digital market to U.S. and European firms, for now, China stands resistant to liberalization, leading to increased tensions with the West and the growing likelihood of internet fragmentation.

As Alibaba, Baidu, and Tencent grow globally from a protected home market of 1.3 billion consumers, it bears considering whether hobbling U.S. firms and leaving the European market wide open to Chinese competitors, who will not be hit by gatekeeper thresholds for many years, is wise at this time. U.S. tech firms might be Europe's "biggest problems" (MEP Andreas Schwab's words) at present, but European poli-

cymakers should fully assess the future of digital markets in Europe if U.S. online platforms are restricted there and Chinese firms are left alone to grow.

In its enthusiasm to constrain U.S. platforms, the European Commission, remarkably, has given no evident consideration to the future of Chinese digital technology firms in Europe under the proposed DMA. China's internet economy has boomed in recent years and, depending on definitions, may be comparable in size only to that of the United States. Services similar to those offered by U.S. online tech platforms, including retail websites, search engines, travel and advertising, audiovisual and computer gaming, online job searches, and mapping services, are flourishing in China. Homegrown Chinese companies enjoy a sanctuary from foreign competition due to market access restrictions imposed by the Chinese government. Estimates are that China **blocks** 10,000 legitimate websites and apps, effectively cutting off billions of dollars in foreign business, including communications, networking, app stores, news and other sites. The cross-border supply of internet services to China is hampered and degraded by this blocking and filtering, regularly making market access for U.S. and European firms impossible.

Human rights is another area of concern. Describing ongoing interventions by the Chinese government in the digital realm, the State Department's 2020 human rights report **lists**:

> arbitrary interference with privacy; pervasive and intrusive technical surveillance and monitoring; serious restrictions on free expression, the press, and the internet, including physical attacks on and criminal prosecution of journalists, lawyers, writers, bloggers, dissidents, petitioners, and others, as well as their family members, and censorship and site blocking.

Europe should not inadvertently support the expansion of these practices—amplified as they are by internet technology—by giving Chinese companies new opportunities to earn additional revenue through the expansion of services to European customers. Of course, market projections of this sort are speculative and difficult to make but, nevertheless, should be attempted before the DMA is approved.

In imposing trade sanctions on imports produced with slave labor, a recent **White House statement** said the People's Republic of China's "forced labor practices run counter to our values as a nation and expose American consumers to unethical practices. They also leave American businesses and workers to compete on an uneven playing field by allowing firms to gain advantage over their competitors by exploiting workers and artificially suppressing wages."

Insofar as Europe agrees with this assessment of human rights violations and unfair labor and trade practices in China, it would be important for the European Commission to analyze whether an expanded presence of Chinese internet companies and digital platforms in Europe will undermine Europe's policy goals in the area of improving trade practices and human rights in China.

## *EU-U.S. Trade and Technology Council*

The **formation** of the EU-U.S. Trade and Technology Council (TTC) announced at the U.S.-EU summit on June 15, 2021, for the purpose, according to a European Commission press release, of leading a "values-based digital transformation of [Europe]" should be a central venue for working through many of the issues raised in this paper. According to the bilateral **summit statement,** the major goals for the TTC include to "seek common ground and strengthen global cooperation on technology, digital issues and supply chains" and "to facilitate regulatory policy and enforcement cooperation and, where possible, convergence." The TTC is **co-chaired** by EU Competition Commissioner Margrethe Vestager, EU Trade Commissioner Valdis Dombrovskis, U.S. Secretary of State

Antony Blinken, U.S. Secretary of Commerce Gina Raimondo and U.S. Trade Representative Katherine Tai. One of the TTC's **main goals** is to "facilitate cooperation on regulatory policy and enforcement and promote innovation and leadership by EU and U.S. firms."

There will be **10 working groups** led by the relevant departments, services, and agencies including: technology standards cooperation (AI and Internet of Things, among other emerging technologies); climate and green tech; data governance and technology platforms; the misuse of technology threatening security and human rights; investment screening; and promoting SME access to and use of digital technologies. In parallel, there will be a **Joint Technology Competition Policy Dialogue** that will "focus on approaches to competition policy and enforcement, and increased cooperation in the tech sector."

Although the organization and subject matter to be addressed by the TTC working groups and the competition dialogue is still preliminary, the issue of online platforms will likely be woven into discussions in all the various working groups. It will be important for officials to discuss policy implications of platform regulations like the DMA in all the relevant working groups. For instance, the working group on promoting SME access to and use of digital technologies will likely involve discussion on the role of large platforms in supporting and inhibiting SME access to digital tools.

As Europe debates the DMA in Parliament, and amendments to antitrust statutes are being considered in Congress, at a time when the G7 has called for coordination on digital issues, it makes sense for U.S. and EU officials to engage in an organized dialogue that will consider concerns about the DMA raised in this paper. It will be important for discussions to proceed in the context of broader announced objectives for digital transformation in Europe and renewed transatlantic cooperation. Indeed, it would be highly ironic if organized bilateral consultations on the proposed DMA did not occur, given the professed objectives of each side and the language of the common summit statement.

An **email**, quoted in the *Financial Times*, from the U.S. National Security Council to the EU delegation in Washington just prior to the U.S.-EU summit lays out U.S. problems with the proposed DMA:

> We are particularly concerned about recent comments by the European Parliament rapporteur for the Digital Markets Act, Andreas Schwab, who suggested the DMA should unquestionably target only the five biggest U.S. firms. . . . Comments and approaches such as this make regulatory cooperation between the U.S. and Europe extremely difficult and send a message that the [European] Commission is not interested in engaging with the United States in good faith to address these common challenges in a way that serves our shared interests. . . . Protectionist measures could disadvantage European citizens and hold back innovation in member-state economies. Such policies will also hinder our ability to work together to harmonize our regulatory systems.

## *Impact of Future R&D Investment in Europe*

While not directly the subject of this paper, a few words should be said regarding R&D capabilities of U.S. online platforms going forward. Given that a principal goal of the TTC is to promote innovation and digital leadership by U.S. and EU firms, the DMA proposal and its potential impact on the strength of U.S. tech champions should be assessed in terms of future private sector support for national security-related R&D and dual-use R&D in Europe. It should be remembered that today U.S. business funds nearly three times as much R&D as the federal government. Technology needed to support national security objectives is reliant on increased collaboration and partnership with leading-edge technology companies that have not traditionally been part of the U.S. government's innovation ecosystem.

According to the **Congressional Research Service**, "some defense experts and policymakers have recognized the shift in the global R&D landscape and the need for [the Department of Defense (DOD)] to rely increasingly on technologies developed by commercial companies for commercial markets." Two of the U.S. companies targeted by the DMA, Alphabet/Google and Apple, together **invested** about €37 billion ($44 billion) in R&D in 2019. Taken in total, GAFAM companies **invested** roughly $70.5 billion in R&D in 2018. The top three European spenders on R&D were automobile companies: Volkswagen, Daimler, and BMW invested a total of €30.3 billion ($36 billion) in R&D in 2019.

In testimony before the Senate Armed Services Committee, then-defense secretary Mattis **stated** that DOD would "leverage commercial research and development to provide leading-edge capabilities to the Department while encouraging emerging nontraditional technology companies to focus on DOD-specific problems." As listed, these include AI; autonomy; cyber capabilities; directed energy; fully networked command, control, and communications technology; microelectronics; quantum science; space; and 5G.50 army futures. As much as large U.S. digital platform companies targeted by the DMA generate outsized sales and profits and possess large cash reserves, it will be important for the TCC to explore partnerships with these firms that could increase innovation and digitization in Europe and contribute to transatlantic security objectives relating to some of the challenges listed by DOD. As the digital economy continues to evolve, it will be important for the United States and the European Union to explore new models of collaboration and partnerships with large online firms that could offer benefits for transatlantic economic security and defense challenges. A focus on promoting the environment for innovation and technology development in Europe will be key to these discussions, and unanticipated impacts of the DMA could negatively affect these efforts.

Urging the TTC leaders to push for specific objectives, a recent statement by Finnish trade minister Ville Skinnari was supportive of identifying methods for increasing R&D. The European Union and the United States should use the TTC to take "a more holistic view" of industrial policy, innovation, and R&D, he said. "In other words, of course we need investments."

## *The Future of the DMA: Next Steps in the European Union*

The DMA is a matter of "**ordinary legislative procedure**" within the European Union and therefore must be jointly agreed to by the European Parliament and the European Council. The European Commission's draft legislation was initially referred to the Internal Markets and Consumer Protection Committee in the Parliament. On June 1, 2021, German MEP and rapporteur Andreas Schwab released a draft report on the DMA proposal, which outlines several amendments to it. As previously mentioned, the Schwab report calls for adjusting the turnover threshold from €6.5 billion to €10 billion, a change that would more precisely limit the reach of the legislation to just U.S. platforms.

Another fundamental change recommended in the Schwab report is an expanded role for national authorities. Amendment 28 (to Recital 77a) states that "national courts will have an important role in applying this Regulation and should be allowed to ask the Commission to send them information or opinions on questions concerning the application of this Regulation." The European Commission would still maintain ultimate authority over the DMA, but the report highlights the goal of increased interventions by national authorities.

In parallel to the European Parliament debates and vote by simple majority, the European Council will deliberate and agree to its negotiating position on the DMA. Then, trialogue negotiations will begin, which involve the Council, the European Parliament, and the European Commission. France, one of

Europe's staunchest proponents of interventionist digital regulation alongside Germany, will hold the Council of the EU presidency for six months beginning in January 2022, meaning the parliament will likely have a sympathetic Council for the expected home stretch of DMA negotiations in Brussels.

Depending on the length and intensity of the legislative review process and the number of amendments, the European Parliament is anticipated to adopt the legislation sometime in 2022, although the earliest implementation would likely occur in 2023. Under this expected timeline, the DMA could have a short implementation phase compared with the GDPR, underscoring the large appetite for swift adoption of digital platform reform rules.

## *Conclusion*

At the U.S.-EU summit, the Biden administration embraced the EU goal of establishing the bilateral **TTC**, which has an ambitious set of objectives. The complexity of the ever-evolving transatlantic digital economy and Europe's relatively poor performance in nurturing global tech champions so far makes concrete progress on transatlantic cooperation and partnership on digital economy issues urgent. In launching the TTC, the United States and the European Union **pledged** to coordinate on shared economic challenges, **including** China's "coercive economic practices." U.S. secretary of commerce Raimondo emphasized the importance of greater coordination on the DMA. Private sector meetings held in conjunction with the summit underscored the importance of commercial collaboration, including on data flows and competition policy.

The DMA proposal is one in a series of initiatives the European Union is implementing to cement its position as a first-mover of standards and agenda-setter for global technology regulation. It cannot be ignored that many in Europe see the DMA package as an integral part of the European Union's **ambitions** for European "technological sovereignty," with the overall goal of building independent, self-reliant systems across a wide range of fields, but particularly in the digital sector.

As French president Macron **has characterized** his intentions, "If we want technological sovereignty, we'll have to adapt our competition law, which has perhaps been too much focused solely on the consumer and not enough on defending European champions."

These are sentiments that could turn out to conflict with the more ambitious cooperative goals of the TTC. Much like the **GDPR**, which was concluded in 2016 and implemented in 2018, the DMA is a far-reaching proposal that stands to have profound **effects** on the digital economy in Europe and on U.S. national tech champions partnering with European innovators and serving European consumers.

As currently proposed, the DMA threatens to impose heavy-handed antitrust measures and to exclusively levy punitive fines on large U.S. firms, while leaving other countries' tech firms—namely European, Chinese, and perhaps Russian companies supplying essentially the same services—untouched. Europe's success in assuming the role of global standards-setter in the area of privacy under the GDPR has energized Brussels, as it seeks further control over the business practices of successful U.S. companies.

With competition policy—as it applies to digital platforms—under review on both sides of the Atlantic, there is a unique opportunity for real collaboration. It is timely to discuss industrial policy regulation, such as the Digital Markets Act, where EU and U.S. approaches are likely to differ. A key element of the TTC should be agreed improvements in the proposed DMA to ensure that basic, multilateral commitments for transparency, due process, national treatment, and nondiscrimination embodied in the WTO continue to be respected by European regulators in the digital space.

***Meredith Broadbent*** *is a senior adviser (non-resident) with the Scholl Chair in International Business at the Center for Strategic and International Studies in Washington, D.C.*

*The author would like to thank* ***William Reinsch, Emily Benson, Jasmine Lim, Catherine Puga, Sarah Mortensen,*** *and* ***Anthony Hokayem*** *for constructive comments and research support.*

*This report is made possible through the generous support of the Computer & Communications Industry Association (CCIA).*