As recently as the 1980s, most U.S. trading partners sought to adopt U.S.-style regulations governing business, manufacturing, and consumer safety. However, the dominance of U.S. regulatory practices in the global tech sector has given way due to the ascendency of the European Commission. Brussels’s growing global regulatory influence marks a tectonic shift: European regulators are increasingly succeeding in demanding changes in the business methods of U.S. tech companies as the price of doing business in Europe, and Europe’s influence is spreading beyond the continent as a result.

Although elements of European tech regulation in the pursuit of digital sovereignty threaten the success of U.S. businesses in global markets, U.S. officials have hesitated to insist on fair treatment in Europe. A case in point is the latest Trade and Technology Council meeting and declaration. Meanwhile, the administration under U.S. president Joseph Biden is bending the language of regulations under the Inflation Reduction Act beyond what Congress intended to accommodate Europe’s objection to discriminatory aspects of the legislation.

Large internet platforms—mostly U.S.-based tech businesses—have led the way in global tech innovation from Web 2.0 to artificial intelligence, despite Europe having a roughly comparable gross domestic product (GDP), population, and talent pool of educated workers. Most game-changing large language models have been developed by U.S. digital services firms competing with one another, not European firms. Even with the success of the light-touch U.S. regulatory environment, Europe believes, to the contrary, that more heavy-handed regulation will nurture the growth of aspirational European tech champions.

Regulatory Costs for U.S. Companies

The EU Data Act makes clear that if Europe intends to impose regulations that slow down U.S.-based tech companies through targeted “gatekeeper” designations and asymmetric data sharing requirements and limitations so that European firms have space to catch up, it will do so.
Europe’s **General Data Protection Regulation** (GDPR) law, implemented in 2018, is shaping data protection laws beyond Europe in countries such as India, Indonesia, and Colombia, which are emulating Europe as the first mover in regulation. The GDPR has caused an 8.1 percent decline in business profits and a 2.2 percent drop in sales, according to a new estimate by researchers at the Oxford Martin School, which is consistent with estimates made before the implementation of the GDPR.

In implementing the Digital Markets Act (DMA) and the Digital Services Act (DSA), Europe is putting in place discriminatory provisions aimed directly at large U.S. platforms. For example, the DSA initially designated 19 entities as Very Large Online Platforms (VLOPs) or Very Large Online Search Engines (VLOSEs), 16 of which are U.S.-based private entities, 2 of which are Chinese, and only 1 of which is based in the European Union. Recently, CSIS published a study estimating the significant economic costs of the DMA, DSA, and other new tech regulations that U.S. and EU companies will bear. For U.S. service providers, the estimated cost of compliance is in the range of $22–$50 billion. CSIS analysis also shows that U.S. global services exports could decrease by 2 percent. Going forward, weighing the steep costs for innovation and productivity against the aspirational benefits of these laws should be a more transparent part of EU deliberations.

While Europe has declined to fix discriminatory provisions in the DMA and DSA, several impactful pieces of legislation still in the drafting stage may be written more in line with international trade obligations of nondiscrimination and national treatment that do not favor domestic businesses to the detriment of foreign firms. Such acts include the **Data Act**, the **European Cybersecurity Certification Scheme for Cloud Services**, and the **Artificial Intelligence Act**. All of these proposed laws deserve attention because of the significant changes they would require in routine U.S. business practices and the attendant impact on U.S exports and jobs.

**The Data Act**

**INTENT**
The overall intent of the proposed Data Act is to achieve more competition in the European cloud services market; give users of connected devices such as cars, refrigerators, and smart phones control over their data, guarding against vendor lock-in (forcing consumers to buy products or services from particular vendors); and enable governments to access data controlled and generated by private companies in emergencies.

EU concern over the lack of European-based data processing service providers, as articulated by EU political leaders, has been clear for some time. U.S.-based companies supply over 70 percent of cloud services in Europe, a figure EU politicians and regulators seek to reduce. According to Margrethe Vestager, executive vice president of the European Commission, “One of the main reasons that U.S. tech companies are popular in Europe is that their products are good. . . . Market forces are more than welcome, but we do not leave it to market forces to have the final say.”

The European Union adopted its overall **European strategy for data** in 2020, which recognizes that data are an essential resource for innovation and economic growth. The document envisions enhancing European competitiveness and data sovereignty by establishing a “single European data space.” The goal of this space is ensuring that **more data are available in Europe** “while keeping the companies...
and individuals who generate the data in control.” Director general for data at the Directorate-General for Communications Networks, Content and Technology (DG Connect) Yvo Volman has said, “Europe should be able to benefit from the value of its industrial data, and we need to act now to make it happen,” which would be transformational for production and manufacturing.

Stretching credulity, the European Commission estimates the new data rules will create €270 billion in additional GDP by 2028. European industrial policy will combine policy, legal actions, and financing mechanisms under an overarching plan to coordinate different elements of the strategy. The Data Act stipulates who must relinquish data—a novel government power as seen from the U.S. side of the Atlantic—as well as who can access data, how data can be used to create value in the European Union, and for what purposes.

The Data Act aims to ratchet up the value of data in the European Union controlled by Europeans, specifically to reduce EU reliance on U.S. companies for data. The regulation targets U.S. tech firms operating in the European Union by forcing the sharing of proprietary data and intellectual property with their European and Chinese competitors. Under Articles 4(3) and 5(8), trade secrets must be disclosed to users and third parties so long as “all specific necessary measures pursuant to Directive (EU) 2016/943 are taken in advance to preserve their confidentiality.” In a world where U.S. trade secrets are regularly lost to theft, enforcing this requirement, particularly on third parties, will prove extremely difficult.

The Data Act stipulates who must relinquish data—a novel government power as seen from the U.S. side of the Atlantic—as well as who can access data, how data can be used to create value in the European Union, and for what purposes.

Industry stakeholders stress that further clarification in these requirements should come out of the trilogue discussions so that data holders have solid guidance on when disclosure of data is mandatory and how to demonstrate when they are likely to suffer damage from the disclosure of trade secrets. Joining this debate, a recent joint statement by Digital Europe and the European Business Roundtable for Industry raised alarm bells regarding what they view as the fundamental interests of holders and creators of industrial data:

Capitalizing on the value of data will be crucial for Europe’s competitiveness over the next decades. But as it stands, the Data Act will force European heavyweights that have invested heavily in automation and digitalisation in sectors like manufacturing, green tech and health to give away their data, leading to a new wave of de-industrialisation and putting our cybersecurity at risk.

**SCOPE**

The scope of the Data Act covers both nonpersonal and personal data. The act defines data as “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording.” Because the Data Act covers all data, not just personal data, it must be read in tandem with the European Union’s **GDPR**, which deals with personal data only.
One of the main obligations of the Data Act is greater accessibility of data generated by product-related services linked to connected devices, such as smartphones and refrigerators. The regulation outlines requirements for business-to-consumer and business-to-business data sharing. Users have the right to request their data and share it with a third party, such as an independent repair service, free of charge and without delay. Furthermore, data holders must make data available to data recipients in a “fair, reasonable and non-discriminatory” as well as “transparent” manner. The regulation enforces users’ right to switch between providers of data processing services.

The draft rules also compel cloud providers to take measures to shield customer data from foreign extraterritorial government data access laws that may (or may not) conflict with EU or national laws on privacy or other EU fundamental rights; intellectual property, including trade secrets; and “the fundamental interests of a Member State related to national security or defence.” To quote Commissioner Breton, “We have also adapted our regulatory framework through the Data Governance Act and the Data Act by inserting anti-Cloud Act clauses, because it is not acceptable that the data of Europeans can be accessed in an unjustified manner.” In some ways these rules are similar to the so-called Standard Contractual Clauses under the GDPR, where the responsibility of sorting out alleged or substantiated conflicts of laws falls exclusively on companies. This recently led the Irish Data Protection Commission to conclude that “any internet platform” subject to the conflicting law, in this case FISA 702, “may equally fall foul” of the data transfer requirements of the GDPR. Similar rules would result in high compliance costs for U.S. tech companies operating in the European Union and push U.S. companies to store more of their data in Europe, further limiting data flows to the United States. The regulation also instructs providers to put safeguards in place to protect international transfers of nonpersonal data. With few exceptions, it broadens the GDPR stance on cross-border transfers of personal data to cross-border transfers of business data.

This will be a challenge for U.S. companies that rely on cross-border data transfers of industrial data and could result in the same levels of disruption and cost that the GDPR caused to U.S. and EU businesses when it was passed in 2018. For example, it seems Tesla would be barred from transferring safety data collected in Europe to analysts at auto manufacturing sites in the United States. In addition, beyond issues of data flows, Article 27 could be used to ban U.S. firms from doing business in some sectoral markets, even if the data is stored in Europe. The article leaves room for interpretations that would lead to the development of “immunity requirements” against non-EU cloud providers—in other words, implementing discriminatory rules against cloud providers subject to foreign laws.

Article 27 could be used to ban U.S. firms from doing business in some sectoral markets, even if the data is stored in Europe.

Contractual Freedom

Intruding into freedom of contracts for data transfers, the regulation also aims to ensure unfair contracts are not imposed on small and medium-sized enterprises (SMEs) through a gray list and a forbidden list of contractual practices. The regulation outlines the requirements for interoperability of data sharing and processing, specifically in a section on the use of smart contracts for data sharing. The European Commission plans to outline models for contractual terms to allow for negotiation.
of fair contracts, as defined by regulators. While U.S. companies will not be obligated to use these templates, they will face pressure to do so to avoid friction and extra scrutiny from EU authorities.

Lastly, relevant parties must make data available to public sector bodies in case of exceptional need. This would be relevant in times of public emergency when certain data are necessary to fulfill a specific task. In these cases, the Data Act might allow sharing of mobility and location information on connected devices for public health and humanitarian reasons. However, U.S. companies may fear handing over proprietary information to their competitors and government agencies. The U.S. Chamber of Commerce commented, “We support frameworks that encourage data sharing when it is in market participants’ mutual interests, but data sharing mandates such as what is envisaged in the Data Act will dissuade companies from investing in R&D or other critical activities in Europe.”

Enforcement of the Data Act will fall to competent member state authorities. There could be fines or financial penalties for infringements of the law, though the European Commission has not yet established revenue-based remedies as under the GDPR. Furthermore, the regulation foresees a dispute settlement mechanism to resolve data-related disagreements.

**Negative Consequences for the European Economy**

Aside from the act’s financial toll on U.S. digital services providers, a rise in digital services costs would pose a high burden for European firms. In a 2022 CSIS survey, over 60 percent of micro and small European firms stated a 5 percent increase in technology costs would be worse or much worse than inflation, slowing demand, or supply chain backlogs. A 2020 EU survey showed how 40 percent of European businesses have a very low level of digital intensity—much lower than their U.S. counterparts. European regulators should recognize that additional digital costs will have an adverse impact on EU economic growth by increasing regulatory compliance costs. Given that European firms are already underinvesting in new technologies and are hampered by higher operating costs than U.S. or Asian firms, increases in the overall cost of digital services in Europe will put European firms at an even greater disadvantage.

The Data Act, as proposed, also may hinder emergence of competitive European platforms by encouraging dependence on easy access to regulated data. While alternative platforms may emerge in the EU market, they would rely inherently on the regulated right to receive ported data. The resulting business models, built around regulation rather than innovation, would make for a less dynamic digital services landscape.

*Given that European firms are already underinvesting in new technologies and are hampered by higher operating costs than U.S. or Asian firms, increases in the overall cost of digital services in Europe will put European firms at an even greater disadvantage.*

As mentioned, the Data Act perpetuates the objectionable classification of gatekeepers designated under the DMA and states that these firms would not be able to use the new portability right established by the Data Act to transfer data to other designated gatekeepers, which discriminates against U.S.-based cloud providers. Thus, U.S. digital platforms, while required to divulge large amounts of data to their competitors upon request, are excluded from receiving the data other firms generate.
On the flip side, preventing European users from migrating their data from one large U.S. provider to another, just because they are large and designated as gatekeepers, runs counter to European consumer interests, including the freedom to benefit from the greater privacy, security, quality, and performance standards U.S. firms often employ. It also runs counter to the principle of interoperability that has characterized the professed goals of earlier EU digital regulations.

The European Union’s attempts to create opportunities for EU companies by preventing gatekeepers from benefiting from the portability right may backfire. For instance, while a given payments company could transfer data from Amazon Web Services to another cloud services company, the recipient could not be another gatekeeper, such as Microsoft. However, the next best option would be transferring the data not to European providers but rather to Chinese firms more efficient than their EU counterparts. Aside from nullifying the goal of the act, this result raises a host of economic security issues. Chinese data providers have a spotty track record when it comes to information sharing. For one, they have blocked some offshore users from accessing business data. Two, they have improperly shared user data with the Chinese government.

**Stakeholder Input on the Data Act**

As ambitious as the Data Act is with its aggressive forays into regulating the new economy, a thorough process for considering stakeholder concerns is important. Stakeholders have had several opposition views. BusinessEurope requested Europe preserve contractual freedom in data sharing. Similarly, the Mechanical Engineering Industry Association (VDMA) maintains that business-to-business data sharing should remain voluntary and authorized on a contract-by-contract basis. In a letter to European officials, German software maker SAP and Siemens offered objections, stating the Data Act “risks undermining European competitiveness by mandating data sharing—including core know-how and design data—with not only the user, but also third parties.” By contrast, the European Consumer Organisation (BEUC) enthusiastically advocates a data portability right for customers that extends beyond personal data.

On February 1, 2023, a total of 30 trade associations released a joint statement stating, “As the policymaking process accelerates on this pivotal proposal, industry warns against possible unintended economic consequences across data value chains.” They also cautioned, “Before opening Pandora’s box, the Data Act’s rules need to be tried and tested in real-world market conditions to make sure that they work for European businesses.”

The exceptional circumstances clause of the Data Act has stimulated further debate. BusinessEurope has expressed concerns about the relatively broad nature of the provision, and the European Data Protection Board and the European Data Protection Supervisor have also questioned the necessity and proportionality of making data available to public sector bodies and EU institutions in these cases.

**Outlook**

The legislative process for the Data Act is about halfway complete, and there is not a clear picture of how it will look in final form. On March 14, 2023, the European Parliament adopted the act, including several amendments, by a vote of 500–23, with 110 abstentions. The final text will be decided through trilogue negotiations involving the European Commission, European Parliament, and Council of the European Union, where many of these issues will be debated.
Overall, member states have supported the Data Act proposal. Finland’s minister of transport and communications expressed that the Data Act was a crucial step in EU efforts to “share knowledge, pool our research and development resources, and ensure that human rights and democratic values are entrenched in all global standards and protocols.” However, the new Swedish president has pointed to challenges in finding agreement on exemptions for SMEs, business-to-government data sharing, and trade secrets.

**Conclusion**

The global influence of European regulators continues to grow despite the better record of the lighter-touch U.S. regulatory model in producing innovation, competition, and growth in technology firms. EU regulations have been directly discriminating against large U.S. digital service providers. The DSA, for instance, designates 16 U.S.-based entities out of the 19 regulated VLOPs or VLOSEs. The Data Act, for its part, is just one element of the European Union's march to digital sovereignty, a multifaceted industrial policy that poses systemic challenges to the future success of U.S. businesses in Europe and global markets.

At present, however, it does not appear Europe is very interested in decelerating its legislative schedule or taking on board policy concerns and questions by U.S. parties with respect to how the Data Act will operate in practice. From the outside looking in, it seems that U.S. officials, so far, have been reluctant to engage with Europe to improve the discriminatory aspects of the Data Act proposal aimed solely at U.S. employers and workers. Now is the time for U.S. digital trade negotiators to vigorously raise questions and concerns with their EU counterparts.

*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.

This report is made possible through generous support from the Computer and Communications Industry Association.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.