2023 Key Threats to Digital Trade

European Union

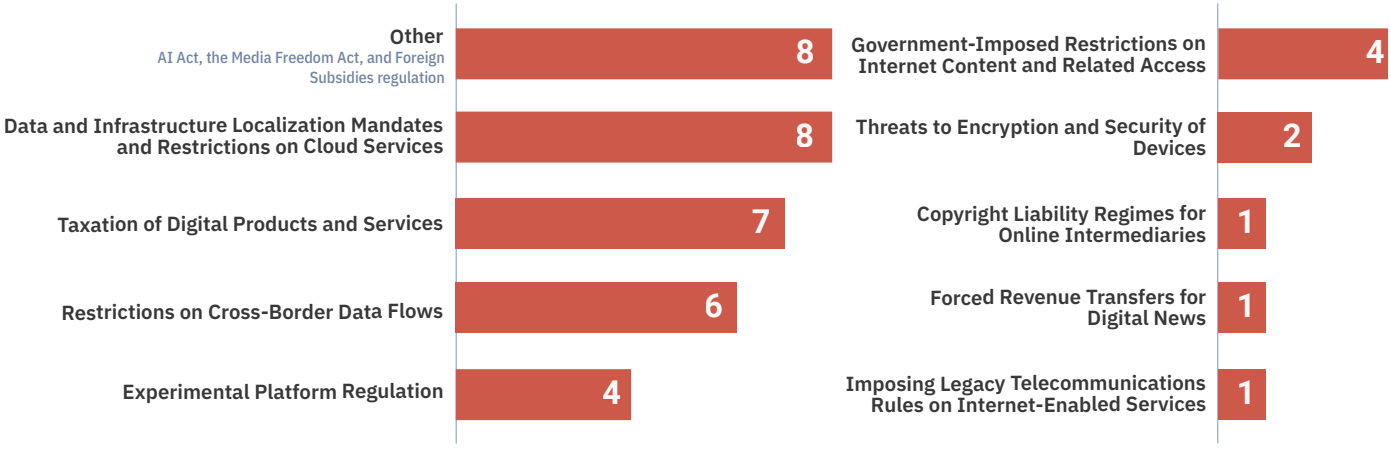
This two-pager accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of February 1, 2024. For the most recent dataset visit digitaltradebarriers.ccianet.org.

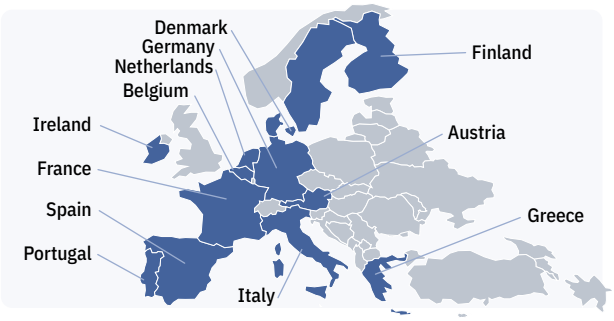
The United States has long enjoyed strong diplomatic and economic relationships with the European Union. The exchange of goods and services has generated widespread benefits for both parties' economies. Digital services in particular are a prominent generator of benefits for U.S. exports in this relationship. The U.S. generated **$186.8 billion in exports of digitally-enabled services** to the bloc in 2022, bringing numerous positive externalities for business operations and consumers in the region and a **trade surplus of $102.5 billion** in digitally-enabled services. (By contrast, that same year, the United States had a deficit in trade in goods with Europe of over $200 billion).

As work is done to advance this relationship through fora such as the U.S.-EU Technology and Trade Council, the United States and the EU should work together to ensure that parties do not restrict the ability of global firms to enter or expand into their markets and engage in cross-border delivery of goods and services.

This engagement comes at a critical moment in the transatlantic relationship. Through its continued pursuit of so-called "digital sovereignty," the EU has enacted policies that hinder the ability of U.S. and other foreign digital services to operate.

Key Threats to the U.S.-EU trading relationship from 2023.[1]





CCIA identified

42

digital trade barriers in the European Union

17 trade barriers enacted

25 trade barriers developing

1 The following is excerpted from CCIA's annual comments submitted to the Office of the U.S. Trade Representative regarding its National Trade Estimate report—first, there are broad takeaways from the region followed by details of the trends identified in the region.

Digital Trade Barrier Trends for the European Union in 2023.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

- The **European Union** Agency for Cybersecurity (ENISA) has built upon protectionist cybersecurity certification standards adopted in France in the EU's Cybersecurity Certification Scheme for Cloud Services (EUCS). A fourth, November 2023, draft of the certification would prohibit companies headquartered outside the EU or owned or controlled by non-EU entities from receiving the highest level of cybersecurity certification; impose stringent data localization requirements; and oblige customer support employees to be located in the EU. One of the scheme's stated objectives is to ensure that the highest level of cloud services is "operated only by companies based in the EU, with no entity from outside the EU having effective control over the CSP, to mitigate risk of non-EU interfering powers undermining EU regulations, norms and values." Organizations which may be required, directly or indirectly, to use an EUCS certified cloud services include: public bodies; over 10,000 "essential entities" regulated under the NIS2 Directive; any number of "important entities" regulated under said Directive; and any other European companies using or contemplating using cloud services regulated under the Data Act. Since the EU has WTO obligations prohibiting discrimination with respect to both government procurement and purely commercial offerings of cloud services it is unclear how such measures could be implemented in conformity with WTO rules.

- Building on the EUCS, the **European Commission** recently announced the launch of new measures to **"de-risk"** Europe's dependence on a wide range of ICT products to strengthen the bloc's "economic security." Although cast generally as a policy of lessening dependence on authoritarian rivals, the policy does not exclude measures disadvantaging U.S. suppliers. Many of those ICT products in the scope of this policy are currently supplied by U.S. companies, and include: microelectronics, including processors, high performance computing, cloud and edge computing, data analytics technologies, computer vision, language processing, object recognition, and quantum technologies. Other potentially critical technologies which the EU may seek to advance its "de-risking" strategy includes: cyber security technologies such as security and intrusion systems and digital forensics, Internet of Things and virtual reality, secure communications including Low Earth Orbit (LEO) connectivity, and AI-enabled systems. For all those technologies, the European Commission seeks to prevent technology security and leakage and the weaponization of economic dependencies and economic coercion, and ensure the resilience of supply chains and the physical and cyber-security of critical infrastructure.

- **ANSSI, the French cybersecurity authority,** has adapted its cybersecurity certification and labeling initiative, SecNumCloud 3.2, to explicitly discriminate against non-French cloud providers in March 2022 as well as over 600 companies that operate "vital" and "essential" services. Problematic requirements include "[t]he registered office, central administration or main establishment of the service provider must be established within a member state of the European Union;" a cap of 24% individual and 39% collective share ownership for non-EU entities; and no veto power for non-EU entities (Article 19.6). The certification standard is no longer entirely voluntary or preferred—tenders have been published with SecNumCloud verification as a requirement. So far, the only two companies that are verified under SecNumCloud 3.2 are French (here and here). An amendment to a recent bill, soon-to-be law, could require all public administrations and state operators (e.g. state-owned enterprises) to use SecNumCloud certified cloud products. Article 10 bis A (IV) provides that a decree will define the terms of application of immunity requirements, including security and ownership criteria. This decree could introduce a broad scope of application for SecNumCloud, particularly regarding capital ownership. The Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique de France (the Ministry of the Economy, Finance and Industrial and Digital Sovereignty of France) has suggested that it could mandate its own SecNumCloud scheme to the broader private sector by defining "sensitive data," and subsequently declaring when SecNumCloud would be required.

Restrictions on Cross-Border Data Flows

- The **Data Act** establishes restrictions on how companies can use commercial and industrial data (e.g., Internet of Things data) generated within the EU as well as additional obligations for large firms operating in local data markets. The Data Act features prescriptive rules on when, where, and how companies should be able to access, process, and share non-personal and personal data with other companies and governments. This includes prohibiting U.S. companies from becoming third parties to receive IoT data in Europe if designated as "gatekeepers;" creating a separate regime for non-personal data, and in practice has the potential to also sweep in personal data, transferred internationally for cloud services providers subject to third party countries' data access requests; obligations to share data that may contain proprietary information; and by potentially empowering national regulators to oversee aspects of the proposal, raising the possibility of duplicative enforcement throughout the 27 member states. Such regulation could leave U.S. companies at a distinct disadvantage compared to Europeans in a constantly innovating and growing IoT market.

- The EU's **Data Governance Act** implements restrictions to the transfer of certain non-personal data held by the public intermediaries to third-party countries, be they data protected by EU trade secrets or intellectual property laws. These restrictions are similar to the General Data Protection Regulation ("GDPR") ranging from "adequacy decisions," consent, standard contractual clauses, as well as an outright ban for sensitive non-personal data. However, the GDPR governs restrictions for personal data, while the DGA extends these obligations to nonpersonal data. The Data Governance Act was enforced starting on September 24, 2023.

- The **updated cybersecurity legislation ('NIS2')** imposes increased security and incident notification requirements as well as ex ante supervision for "essential" service providers (e.g., cloud providers, operators of data centers, content delivery networks, telecommunications services, Internet Exchange Points, DNS). It entered into force on January 16, 2023, and must be transposed into national law by each member state by October 17, 2024. The legislation includes the obligation for such providers to be certified against an EU certification scheme to be developed under the EU Cybersecurity Act ("CSA"). The NIS2 Directive will also intensify reporting requirements and punishments. The first EU cybersecurity scheme under development relates to cloud services which feature discriminatory requirements against U.S. providers.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

In response to a campaign from incumbent European telecommunications providers, the European Commission launched an exploratory consultation in February 2023 asking for input on the suggestion that "large traffic generators" should make financial contributions, termed "network usage fees," to European telecommunications network operators to support network deployment. The incumbent telco association ETNO suggests that large U.S. content and application providers (CAPs) should be required to pay fees to European ISPs for the content demanded by the ISPs' customers.

ETNO's proposal is discriminatory by nature and in evident contrast with the net neutrality principle, as it leaves the door open to discriminatory behaviors of incumbent telcos, who could throttle or block internet users' access to specific services in case of lack of agreement with content providers. In addition, there is growing evidence that telcos have successfully accommodated growing traffic from content and application providers (the source of demand for their services) with relatively little additional network investment. The telco incumbents estimate that total payments could amount to 20 billion euros annually, i.e., more than four times the amount discussed under the abandoned EU Digital Services Tax proposal.

The proposal of the incumbent telecommunications providers has been challenged by some member states, seven of whom suggested slowing down the process to avoid unintended consequences of implementing a SPNP requirement, and several others echoed those concerns mid-2023. In October 2022, the body of European telecom regulators (BEREC) stated that it "has found no evidence that such mechanism is justified" and warns that the proposal "could be of significant harm to the Internet ecosystem." In its response to the European Commission's consultation, BEREC reiterated its opposition to the proposal and also maintained that "in the case of such payments, the termination monopoly of the ISPs is reinforced, therefore increasing the bargaining power for ISPs. ISPs may [thus] be in a position to discriminate and self-preference own services".

The Commission released a summary of the responses received in the public consultation in October 2023, where it was documented that a majority of respondents opposed any mandatory funding mechanism. Arguments against the proposal focused on the inconsistency with net neutrality principles, the harms it would impose on innovation, and the damage it could bring for competition and consumers (such as a decrease in the range of content available and/or higher prices for internet services). However, industry is concerned that the Commission has signaled an intent on imposing network usage fees regardless of this finding. The Commission deemed the consultation results "not conclusive" on the question of implementing network usage fees (despite the overwhelming opposition) and EU Commissioner Thierry Breton said that "Europe will do 'whatever it takes' to keep its competitive edge" including by "finding a financing model" for the EU telecommunications industry, potentially through new legislation (such as a "Digital Networks Act"). In this context, Commissioner Breton convened a roundtable with representatives of the financial sector to discuss how to attract more private investment in connectivity infrastructure in December 2023.

The Commission's published work plan for 2024 hints at further work on the issue of connectivity and network infrastructure: "Following the recent exploratory consultation, we will prepare the ground for possible policy and regulatory actions regarding Digital Networks and infrastructure, notably to facilitate cross-border infrastructure operators in the Single Market, accelerate deployment of technologies and attract more capital into networks."

In accordance with the work plan, on 21 February 2024, the European Commission is expected to present a Connectivity Package on Europe's digital infrastructure. The package will include a recommendation on subsea cables infrastructure, as well as a White Paper on the future of connectivity. The white paper will focus, among others, on the creation of pan-European telecom operators and on the upcoming review of the European Electronic Communications Code (EECC). The EECC already features a dispute resolution mechanism over interconnection agreements which is limited to contractual disagreements between telecom providers and online communications services (Articles 26 and 60 EECC). Should the white paper suggest broadening the scope of this mechanism to other players, it could reopen the 'fair share' debate by the back-door.

The United States cautioned the EU to "avoid discriminatory measures that distort competition" and argued that "it is difficult to understand how a system of mandatory payments imposed on only a subset of content providers could be enforced without undermining net neutrality" in its filing before the European Commission. The United States and partner nations rejected this proposal when advanced by the European Telecommunications Network Operators' Association (ETNO) a decade ago.

Taxation of Digital Services

Digital services taxes (DSTs) are gross-based taxes that originated in Europe and target a small number of primarily U.S.-based companies, while excluding most European and foreign rivals from scope. Despite efforts to repeal and replace these measures with a principles-based approach negotiated at the OECD, a number of DSTs remain in place in France, Italy, Spain, Austria, Hungary, and the UK. In France alone, the Finance Minister recently calculated that the DST will have increased French tax revenue by over 2.3 billion euros through 2023, primarily by expropriating revenue from U.S. companies and the U.S. tax base (and subjecting U.S. firms to double taxation).

Given slow progress in the OECD, there is an ongoing threat of new digital taxes across the European Union. DSTs undermine the international tax system, expose companies to extensive double taxation and increase costs for consumers.

Further, other sources of taxation on digital services threaten to impose overlapping financial burdens on U.S. providers operating in the region. For example, since 2017, France has imposed a tax on video content, on streaming services, and video-sharing websites ("TVC") that supply content in France on a cross-border basis. Industry reports that the taxes are primarily being collected from U.S. companies and the funds go towards subsidizing the production of original French content and programming through the French National Film Fund (CNC). The tax was originally called the "YouTube tax." Suppliers subjected to the TVC also pay corporate income tax and the French DST, leaving U.S. suppliers facing double and, in some cases, triple taxation. The French government is now considering the possibility of introducing a new tax on streaming music services with a similar goal of using revenue from foreign companies to subsidize original French content, leaving industry concerned of a new discriminatory taxation revenue stream that could leave U.S. services paying four streams of taxation, with several serving as cross-subsidies for local industries.

Digital Services Act

The Commission proposed a **"Digital Services Act" (DSA)** entered into force on November 16, 2022. The Digital Services Act took effect in 2023 for firms designated as "very large online platforms" and "very large search engines", and will apply to all other services on February 17, 2024. These new rules will police how providers moderate for illegal content, counterfeiting, collaborative economy services, or product safety.

The DSA imposes a range of new due diligence obligations including 'know your business customer' and transparency of content moderation, and cooperation with authorities. Large platforms, notably U.S. companies will have to comply with additional obligations such as strict transparency and reporting obligations, yearly audits, obligations to disclose the main parameters used in their recommendation systems, and requirements to appoint a compliance officer. Fines can reach up to 6% of annual turnover. Further, "very large online platforms and very large search engines"—defined as those with 45 million active users or more in the EU— only have 4 months to comply with the new regulations, while most companies receive 15 months to prepare. The European Commission designated on April 24, 2023, the very large online platforms and search engines. Out of the 19 services designated, 17 are U.S. firms, and only one firm is European. Since many of the most egregious distributors of harmful content are smaller operators, the wisdom of focusing the most prescriptive requirements on an arbitrarily-defined set of larger operators is highly questionable. A second designation was made on Dec. 20, 2023, to require three adult content websites to follow the DSA's obligations as VLOPs.

The DSA was also weaponized as a means to incorporate regulations on a variety of other topics not initially germane to the stated goal of online safety. For example, the inclusion of restrictions on personalized targeted advertising undermines the horizontal normative purpose of the DSA proposal and harms European companies along with U.S. firms.

Throughout the implementation, the European Commission continues to use the DSA to further regulate online services and potentially deviate from other legislations. As the European Commission is building a database to collect the statement of reasons sent by online platforms to their users, further information than DSA requirements were asked to online services.

Online marketplaces, including a large number of U.S. companies, are now required to obtain and verify extensive information on traders before allowing them to reach consumers. Such requirements, backed by high fines, incentivize marketplaces to limit and/or to take down traders, meaning fewer products available online. Some categories of products considered too risky, could even be dropped.

Experimental Platform Regulation

In recent years, U.S. technology firms have identified a rise in protectionism implemented through targeted regulation against U.S. firms.

The **Digital Markets Act (DMA)** was adopted by the European Parliament and the Council of the EU on September 14, 2022. The measure entered into force on November 1, 2022, and took effect on May 2, 2023. Under the rules, companies that operate a "core platform service" must notify the European Commission upon meeting pre-defined thresholds for European turnover, market capitalization, and number of European end and business users. These thresholds have been carefully designed to primarily capture U.S. technology companies, reflecting some policymakers' intent to shield European operators and burden foreign (mainly U.S.) firms. The list of "core platform services" furthermore carves out business models of large European rivals, both digital and not, in media, communications, and advertising. As of October 2023, the European Commission has designated six companies as the so-called "gatekeepers" under the DMA, subjecting 22 of their services to the new rules. Five out of those six companies (the sixth is Chinese) and 21 of the 22 services are American.

Starting from March 7, 2024, companies designated as the gatekeepers, in relation to their designated core platform services, will be prohibited from engaging in a range of business practices that are generally procompetitive (e.g., offering consumers integrative efficiencies). Furthermore, the Commission will be authorized to micromanage future digital innovations, product integrations, and engineering designs of U.S. companies. The DMA will also in some cases compel the forced sharing of intellectual property, including firm-specific data and technical designs, with EU competitors, effectively requiring U.S. firms to subsidize their EU rivals. In this sense the DMA represents a dramatic shift in competition enforcement, resulting in greater potential infringement on fundamental intellectual property rights and freedom to contract, previously only exercised in exceptional circumstances. Unlike traditional competition enforcement, the Commission will be able to impose these remedies without an assessment of evidence of harm, without taking into consideration any effects-based defenses, and without considering procompetitive justifications put forth by the targeted companies. While ostensibly designed to address conduct presumed, in a specific context, to be harmful, the concept of "gatekeeper" has been extended to unrelated EU regulations including the Data Act.

The "gatekeeper" designation has also emerged as a method to discriminate against U.S. firms in the nascent realm of open banking, detailed below.

Regulations on Artificial Intelligence

In April 2021, the European Commission proposed the AI Act to regulate artificial intelligence (AI) across all sectors. The objective is to support AI in the EU and protect EU citizens. The EU Member States and European Parliamentarians reached a political agreement at the end of 2023. The final text of the agreement was agreed upon in January 2024 and will need to be officially adopted by EU Member States and the European Parliament in the coming months. The regulation may apply as early as 2025 in all 27 EU Member States.

Lawmakers see the AI Act as an opportunity to set global norms: like GDPR, the AI Act would be a first-of-its-kind regulation, with the potential to carry soft influence worldwide as businesses adapt to EU-specific requirements, and to inspire AI regulation in other regions. EU lawmakers decided to align the AIA definition of the OECD definition to ensure international alignment. The EU proposes to regulate these systems by risk level: (1) low-risk systems are subject to transparency rules; (2) high-risk systems must comply with a comprehensive regulatory regime including numerous requirements such as conformity assessments, auditing requirements, and post-market monitoring; and (3) prohibited systems pose unacceptable risk and are banned. In addition, providers of general-purpose AI models will be subject to specific transparency rules, including in the area of copyright.

Providers of general-purpose AI models with systemic risks will be subject to stringent requirements, including adversarial testing and cybersecurity requirements, as well as risk assessments and mitigation obligations. The law will apply to both providers and users of AI systems where the "output" of that system is used in the EU. Fines can reach up to 6% of annual global turnover.

Elements of this legislation that may impede the development and use of AI in Europe include: unclear definitions, burdensome requirements for general-purpose AI models; classification of what constitutes high-risk and prohibited AI; and unclear allocation of responsibilities for actions in the AI value chain. The broad definition of so-called "high-risk" applications, cumbersome compliance requirements and steep fines, will create new compliance burdens for U.S. companies doing business in the EU. Additionally, the vague wording of certain prohibited systems risks banning low-risk applications, such as biometric categorisation to mitigate bias.

Further, the expansive definition of "high-risk" in the legislation could dampen innovations and create significant legal uncertainty for both developers and implementers. A burdensome conformity assessment process could apply for products and services that are already subject to a multitude of regulatory mandates. Compliance requirements for "high risk AI" are not only administratively cumbersome but may also not be technically possible for firms to adhere to with certainty. For example, instituting an unclear division of responsibility between AI developers ("providers") and deployers ("users") may render use of AI, in many cases, infeasible.

As part of the ongoing final negotiations on the Artificial Intelligence (AI) Act, European member states and Parliament agreed on a two-tiered approach to general-purpose AI model regulation. A first layer of obligations would apply certain obligations—such as documentation, the sharing of training content and testing—on providers of general-purpose AI models. A second layer would, on top of the first layer, impose stricter obligations on providers of general-purpose AI models with systemic risks. The threshold for making a distinction for the second layer of additional regulation was set at 10^25 FLOPs (floating-point operations per second), and the European Commission was granted vast powers to designate models below the threshold based on vague criteria. The approach in itself is fundamentally flawed, arbitrary, and is expected to disproportionately impact U.S. foundation model developers.

Finally, imposing stringent requirements on cutting-edge technologies and essential building blocks, such as general-purpose AI model, departs from the AI Act's original risk-based approach and is likely to disproportionately impact developers of such systems (as opposed to implementers, the more logical target). The decision to impose a two-tiered AI regulatory framework whereby the most stringent obligations focus only on the largest general-purpose AI model developers could disproportionately impact and discriminate against U.S. companies.

Payment Services and Open Finance Package

On 28 June 2023, the European Commission unveiled its open finance and payments package, an effort to modernize payments regulations and better promote "fintech." The package includes 3 legislative initiatives: a proposal for regulation on a framework for financial data access (FIDA), opening up third-party access to financial data (such as mortgage, credit and savings account, savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate, etc.); a proposal for a Directive on payment services and electronic money services (PSD3), containing rules concerning licensing and supervision of payment institutions; a proposal for a Regulation on payments services (PSR), containing the rules for payment services providers providing payment and electronic money services and including rules on the promotion of open banking - the development of standard interfaces allowing service suppliers, when authorized by an account holder, to facilitate direct access to a bank account for the purpose of access to account information—e.g. connecting multiple bank accounts to a single interface or connecting to a budgeting app (personalized budgeting advice, expense tracking, and financial management tools).

At the end of 2023, during efforts to finalize the PSR and FIDA regulations, the European Parliament sought to link the regulations to the Digital Market Act concept of "gatekeeper," specifically denying the benefits of the amended regulation (i.e., access to standardized interfaces for account and financial data information) to any company designated under the DMA as a “gatekeeper.” Given the absence of any competition-related analysis motivating the introduction of these amended rules, transposing the concept of gatekeeper to a new and unrelated sector appears both arbitrary and unwarranted.

While the amendments are still under discussion, the introduction of discriminatory blanket prohibitions will severely limit consumer choice in the EU; cement incumbents' privileged position and hamper competition and innovation in the payment sector; run counter the EU’s international trade commitments.

Excluding U.S. companies from offering innovative services on the same terms as European and third-country competitors (and in sectors dominated by larger incumbents) is contrary to the objective of fostering greater competition.

The European Parliament and EU Member States are expected to adopt their respective positions in the first half of 2024 before entering negotiations in view of finding an agreement before the end of this year.