KEY THREATS TO DIGITAL TRADE 2022

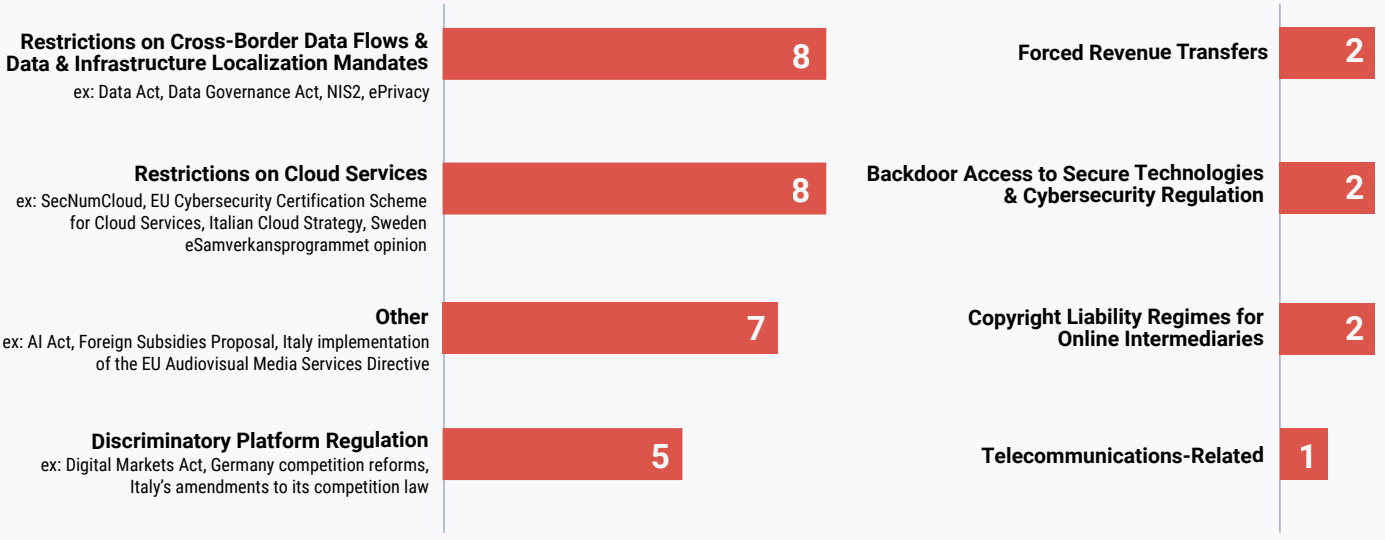
The European Union

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 **$230.9 billion in exports of digital services** to the region in 2019, bringing numerous positive externalities for business operations and consumers in the region and a **trade surplus of $86.5 billion** in just BEA-identified Potentially ICT-Enabled Services.

As work is done to advance this relationship through fora such as the U.S.-EU Technology and Trade Council, the U.S. and 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 pursuit of so-called "digital sovereignty", the EU has enacted policies that hinder the ability of U.S. digital services to operate. 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.

Key Threats to the U.S.-EU trading relationship in 2022



CCIA identified **40** digital trade barriers in the European Union

19 policies have been enacted

21 are in development

Digital Trade Barrier Trends for the European Union in 2022

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

- The **Data Act**, introduced in February 2022, seeks to build on other digital market regulations such as the Digital Markets Act and Digital Services Act to establish restrictions on how companies can use personal, commercial, and industrial data generated within the EU as well as additional obligations for large firms operating in local data markets. The Data Act proposal features new prescriptive rules on when, where, and how companies should be able to access, process, and share data with other companies and governments. This includes prohibiting U.S. companies from becoming third parties to receive IoT data—both personal and non-personal—in Europe if designated as "gatekeepers"; potentially creating a separate regime for non-personal data transferred internationally for cloud services providers regarding third party countries' requests for access to non-personal data; obligations to share data that contains 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.

- The EU's **Data Governance Act** implements restrictions to the transfer of certain non-personal data held by public and private 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 ranging from 'adequacy decisions', consent, standard contractual clauses, as well as a potential outright data transfer ban for sensitive non-personal data. However, the GDPR governs restrictions for personal data, while the DGA extends these obligations to non-personal data for those public and private intermediaries.

- The **updated cybersecurity legislation ('NIS2')** will impose 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). The legislation is at an advanced stage, with the European Parliament and EU Member States reaching a political agreement on the legislation in May 2022. The legislation would include 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 would 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 as described in the section above.

- The EU also has been working on amending the existing **ePrivacy Directive** and proposed the "ePrivacy Regulation" in 2017. The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including over the top services. Rules that were originally created for traditional telecommunication services would then apply to a variety of online applications from those that provide communications and messaging services to personalized advertising and the Internet of Things.

Restrictions on Cloud Services

- ANSSI, the **French** cybersecurity authority, has adapted its cybersecurity certification and labeling initiative, SecNumCloud, to explicitly discriminate against non-French cloud providers. 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. The certification standard is no longer entirely voluntary or preferred—tenders have been published with SecNumCloud verification as a requirement. The only companies that are verified under SecNumCloud are French. 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 further refining the notion of "sensitive data", and subsequently declaring when SecNumCloud would be required. An existing definition of "sensitive data" includes all personal data of all French citizens, industrial and company data, and any data related to French public servants.

- 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 draft of the certification with "high assurance level" includes data localization requirements within the EU; prohibition for non-EU entities to own, in part or in whole, or operate cloud services in the EU; obligation for customer support employees to be located in the EU; and a stated objective of cloud services providers being "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."

- The **Italian** Cloud Strategy (September 2021) bears many similarities with the French strategy. However, it also explicitly requires the storage and processing of encryption keys in Italy for certain categories of data. This requirement will apply for any certified (or 'qualified') commercial cloud services that may be used to host local and central administrations' "critical" and "strategic" data and services. The Strategy also implies the advent of national localisation requirements for other data and services, beyond encryption keys. The roll-out of a new National Strategic Hub, made of at least 4 data centers "geographically distributed throughout the country", will "offer (...) licensed private / hybrid cloud and qualified private cloud services". It "will [also] be entrusted to qualified national providers" to host, e.g., "encryption tools integrated on a Public Cloud". The definitions of "critical" and "strategic" data and services have been decided by the Italian national cybersecurity agency and the Department for Digital Transformation through subsequent implementing regulations.

- Additionally, the use of U.S. cloud service providers has decreased in **Sweden**. In October 2018, eSamverkansprogrammet, a quasi-governmental organization, published an opinion that concluded, due to the extra-territorial reach of U.S. law enforcement authorities, that the use of U.S. services would conflict with EU and Swedish law.

Network Fee Legislation

- In response to a campaign from incumbent European telecommunications providers, the European Commission announced its intention to launch a public consultation in December 2022 or early 2023 to consider a **'Sending-Party-Network-Pays' (SPNP)** model for Internet traffic. This is similar to the regulatory model being expanded upon in South Korea, the effect of which (as in the EU) would be additional fees assessed predominantly on successful U.S. firms, whose content and applications have attracted significant foreign demand. The United States and partner nations rejected this proposal when advanced by the European Telecommunications Network Operators' Association (ETNO) a decade ago.

The initial ETNO report and proposal is discriminatory by nature and in evident contrast with the net neutrality principle, as it leaves the door open to discriminatory behaviours 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. This suggests that this initiative is simply a strategic attempt to leverage anti-tech sentiment for commercial gain, by obtaining governmental sanction for creating a new tollbooth to access to their customers. Several EU member states have expressed backing for the telecoms' campaign; in foreshadowing the upcoming consultation, EU Commissioner for the Internal Market Thierry Breton said, "We also need to review whether the regulation is adapted with the 'GAFAs' (Google, Apple, Facebook, Amazon) for example, which use bandwidth (provided by) telecom operators."

Government-Imposed Restrictions on Internet Content and Related Access Barriers

The European institutions adopted on 19 October 2022 a **"Digital Services Act"** (DSA), which will further depart from transatlantic norms on liability for online services. These new rules will police how providers moderate for illegal content, counterfeiting, collaborative economy services, or product safety.

The DSA imposes new obligations such as due diligence obligations: notice & action, 'know your business customer', transparency of content moderation, and cooperation with authorities. Large platforms, notably U.S. companies, having 45 million active users, will have to comply with additional obligations such as strict transparency and reporting obligations, yearly audits, disclose the main parameters used in their recommendation systems, and appoint a compliance officer. Fines can reach up to 6% of annual turnover. Further, "very large online platforms"— defined as those with 45 million active users or more in the EU—will only have 6 months to comply with the new regulations, while most companies receive 15 months to prepare. The European Commission will commence designation of VLOPs on Feb. 16, 2023. The European Commission will commence designation of VLOPs on Feb. 16, 2023.

The DSA was used 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. Online marketplaces, including a large number of U.S. companies, could become liable for every product sold through their channels. As such, online marketplaces will have to adopt a very cautious approach, especially with the high fines set out in the DSA. In case of doubt, online marketplaces would be incentivized to take down products, meaning fewer products would become available online.

Discriminatory Platform Regulation

In recent years, U.S. technology firms have identified concerns around a rise in protectionism relating to digital competition in the form of targeted regulation and increased antitrust actions against U.S. firms.

The **Digital Markets Act** (DMA) was introduced in December 2020. The European Commission reached a political agreement on implementation for the Digital Markets Act in March 2022 and the European Parliament formally adopted it in early July. The rules have entered into force and the first companies are expected to come into compliance early 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 consumer users and business users.

These thresholds have been set at levels where primarily U.S. technology companies will fall under scope, reflecting some policymakers' intent to ensure that only U.S. firms fall under scope.

Once under the scope of the DMA, companies will be prohibited from engaging in a range of pro-competitive business practices (e.g., integrating products and services to improve user quality). Furthermore, the Commission will be vested with gatekeeping authority to approve 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, and could even require building new technical infrastructure to benefit rivals, effectively requiring U.S. firms to subsidize rivals. In this sense the DMA represents a dramatic shift in competition enforcement, resulting in greater governmental encroachment on fundamental intellectual property rights and freedom to contract. Unlike traditional competition enforcement, the Commission will be able to impose these interventions without an assessment of economic evidence, without taking into consideration any effects-based defenses, and without considering procompetitive justifications put forth by the companies targeted. It is concerning that this DMA "gatekeeper" designation is now being extended into new EU regulations including the Data Act.

Additionally, some European countries have pursued *ex ante* competition approaches that restrict U.S. firms ability to offer services in the region. These examples include:

- **Germany** recently reformed its competition rules to target companies of "paramount significance for competition across markets", which came into force in January 2021. The intention of this reform is to make it easier to sanction large digital companies, with provisions that effectively reverse the burden of proof for finding the abuse of a dominant position against companies deemed to be of "paramount significance", and eliminates the Higher Regional Court of Düsseldorf from the appeals process which otherwise normally applies to defendants.

- **Italy** amended its competition law to create a presumption the business users are economically dependent on digital platforms that provide them services, which implies new obligations and liabilities exclusively for these digital services.

- The **Belgian, Dutch, and Luxembourg** competition authorities proposed amendments to their competition regimes allowing for the imposition of remedies without proving harm to consumers for digital companies. This will increase legal uncertainty and open a path to use competition to slow down successful U.S. companies operating in these regions.