Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 144

The Rise of Digital Protectionism? EU-US Comparative Perspectives and Avenues of Collaboration

Nikolaos Theodorakis & Dimitra Tzeferakou

2025

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Nikolaos Theodorakis is a Partner in the London and Brussels offices of Wilson Sonsini Goodrich & Rosati, where his practice focuses on privacy and cybersecurity. Nikolaos regularly counsels on matters of EU data protection law, GDPR compliance, UK GDPR preparedness, cybersecurity, advertising, and marketing and offers a full cycle of services that includes both non-contentious matters and investigations with supervisory authorities. In addition, Nikolaos is an associate professor of law at the University of Oxford (UK), an assessor at the University of Cambridge (UK), and a TTLF Affiliate at Stanford Law School, focusing on technology and intellectual property issues. Previously, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. He also gained professional experience at the U.S. Committee on Capital Markets Regulation, the Kluge Center at the U.S. Library of Congress, and the UK Ministry of Justice. Nikolaos has received awards from several bodies, including the State Council of the People's Republic of China, the UK Economic and Social Research Council (ESRC), British Academy, and the Greek Parliament. He has served as a consultant and a legal trainer for the United Nations Interregional Crime and Justice Research Institute (UNICRI), a consultant for the Organisation for Economic Co-operation and Development (OECD), an expert and rapporteur for the International Academy of the Belt and Road, an assessor and peer reviewer for Transparency International, and other international institutions and organisations.

Dimitra Tzeferakou is a Harvard University Master's Degree candidate and a Dean's Scholar at Harvard Medical School, focusing on issues of AI law, medical and pharmaceutical law, medical ethics, genetics & genomics, intellectual property, and data protection. Ms. Tzeferakou is an Attorney-at-Law, qualified in Europe and RFL in England & Wales. She has been advising at the forefront of the new EU AI Act, and has delved into matters of fundamental human rights and AI. She represents companies of all sizes and sectors, with a particular focus on technology companies. Ms. Tzeferakou has prior work experience at the Council of Europe, the Greek Parliament, a healthcare company, and leading law firms. Ms. Tzeferakou holds a bachelor's degree in politics, a bachelor's degree in law, as well as an LL.M. and an M.Sc. degree. Her thesis on the conduct of clinical trials during pandemic conditions has received a first-class honor from the Athens Medical School. Ms. Tzeferakou has published several research papers, and has participated in numerous conferences and round tables around the world as a convenor or a moderator. Ms. Tzeferakou is an associate MCR at Wolfson College, University of Oxford. She has conducted research, and has been a research assistant, in the United States, Germany, Switzerland and Belgium.

General Note about the Content

The opinions expressed in this paper are those of the authors and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos Theodorakis & Dimitra Tzeferakou, The Rise of Digital Protectionism? EU-US Comparative Perspectives and Avenues of Collaboration, Stanford-Vienna TTLF Working Paper No. 144, http://ttlf.stanford.edu.

Copyright

Abstract

Digital protectionism, characterized by the adoption of policies and regulations that prioritize national interests in the digital economy, is becoming increasingly prevalent in both the European Union (EU) and the United States (US). This trend reflects broader geopolitical, economic, and technological shifts. Measures such as data localization requirements, data transfer restrictions, and stringent privacy provisions, are reshaping the global digital landscape. This paper will explore the potential rise of digital protectionism in the EU and the US, analyzing its drivers and implications for global digital governance. In the EU, digital protectionism often takes the form of stringent privacy laws like the General Data Protection Regulation (GDPR), data sovereignty initiatives, and legislative efforts like the Digital Markets Act (DMA) and the Digital Services Act (DSA). These measures are frequently seen as aiming to curtail the dominance of non-EU tech giants. In the US, digital protectionism manifests primarily through measures such as export controls on advanced technologies, increased scrutiny of foreign investments in critical tech sectors, and state-specific privacy laws. The paper will define and conceptualize digital protectionism in the context of modern regulatory frameworks, identify legal and policy measures that reflect protectionist trends in the EU and the US, and analyze the implications of digital protectionism for international trade and innovation.

Table of Contents

1. Introduction

1.1.Framing the Debate

The digital economy has quickly risen to become a central arena for geopolitical negotiation and competition. Governments around the world are increasingly introducing measures that could broadly fall within the realm of "digital protectionism". Digital protectionism colloquially refers to policies that prioritize domestic control over data, valuable technological assets, infrastructure and markets. Naturally, this occurs as the flip side of openness and free trade. In dissecting digital protectionism, we will first discuss traditional protectionism, which is a trade restrictive policy that most nations globally have been pursuing for the majority of their commercial activity throughout centuries. Trade protectionism can take various forms, including tariff-related measures (e.g. duties and tariffs on imported goods) and non-tariff measures (e.g. import quotas, licensing requirements, technical barriers to trade etc.). Non-tariff measures are generally more difficult to detect, and consequently harder to litigate before the World Trade Organization (WTO), claiming that a country is violating the WTO rules.

Although when we refer to trade protectionism most people instinctively think of duties and tariffs, the majority of trade restrictive measures nowadays are more nuanced, technically complicated, and difficult to detect. For instance, the WTO has published statistics arguing that most countries

pursue non-tariff barriers to trade.[1] Analysts may consider this counter-intuitive, since the post-2000 era is generally considered an era of free trade. However, trade protectionism has always, and consistently, existed throughout human history. There is no single country or economy that can claim it is following an entirely free trade policy in every segment of its economic activity. As such, trade protectionism has experienced times of rising or declining popularity- the recent years are a testament to increasing popularity for trade protectionism in traditional economic activity.

Before we move to further define digital protectionism and investigate how it is manifesting in the EU and the US, we will briefly discuss why countries have historically relied on trade protectionism. There are several arguments that can be used in favor, or against trade protectionism, yet when focusing on the former, academic literature has recurring arguments including infant industry protection, national security, and domestic policy reasons.

Infant industry relates to the notion of protecting a domestic industry that is still in the rise, and therefore needs a protected status until it is nourished and grows to the extent that it can compete internationally. For instance, let's assume that a country wants to invest in its semiconductor production. If it were to simply start competing internationally, without any protectionist measure, this would likely be a failed venture since other countries already have a head start, and will be significantly more competitive when producing and selling microchips. This will result in several inefficiencies, and the microchip industry will not be able to take off since it is practically

[1] World Trade Organization. (n.d.) Understanding the WTO: The Agreements — Non-tariff barriers: red tape, etc. Available at: https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm9_e.htm (Accessed: 30 October 2025).

impossible to compete freely with other more advanced manufacturers who possess the know-how and the selling strategies to optimize their production through economies of scale.

To address this dead-end of not being able to enter a new market/industry, countries often introduce protectionist measures to safeguard their infant industry of choice. This typically includes a blend of measures such as tax reliefs, investment incentives, friendly regulatory framework, and subsidies to endorse domestic production, as well as duties and other technical barriers against foreign microchips. These two joint initiatives, incentives for domestic production and roadblocks for foreign imports, creates a dynamic and powerful policy mix that can protect the local economy and significantly boost domestic production. Through a thoughtful industrial policy, countries can develop a targeted sector, and open up to free trade once the industry has grown enough to be internationally competitive. Naturally, the right timing is a particularly delicate matter since, if the protectionist measures retract too early and while the industry is still immature, one risks losing all the progress made as it will not be possible to compete internationally. Conversely, it is extremely challenging to untangle the protectionist measures once they are introduced and the industry is comfortable receiving the incentives and benefits. In fact, a key issue with trade protectionism is that once protectionist measures are introduced, they create dependencies, which are extremely difficult to address, also for political reasons. As a result, industries end up being heavily subsidized in the long-run, and governments are unwilling or hesitant to withdraw their support. Ultimately, this leads to market distortion and economic inefficiencies since the former infant industries expect the government to intervene and assist them as needed.

Considerations surrounding national security have been increasingly prevalent in the recent years. For instance, the United States invoked Section 232 Tariffs (Steel & Aluminum) where it imposed tariffs on steel, aluminum etc. citing national security concerns.[2] The affected members have argued that these measures violate WTO rules, including when the United States imposed duties on steel products from China citing national security concerns, a case that eventually reached the WTO.[3] The complaining parties include Canada, China, and the European Union, which have argued that Section 232 measures, along with exemptions from the applications of these measures, violate the US obligations under the WTO. GATT Article XXI's on national security exception provides, in relevant part, the following: "*Nothing in this Agreement shall be construed. . . .(b) to prevent any [member country] from taking any action which it considers necessary for the protection of its essential security interests: (i) relating to fissionable materials or the materials from which they are derived; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment; (iii) taken in time of war or other emergency in international relations; or (c) to prevent any [member country] from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security*." When invoking the national security exemption, the US argued that these

[2] Murrill, B.J. (2018) *The "National Security Exception" and the World Trade Organization.* Legal Sidebar, CRS Product No. LSB10223. Congressional Research Service. Available at: https://www.congress.gov/crs-product/LSB10223 (Accessed: 30 October 2025).

[3] Staiger, R.W. (2023) *Will the National Security Exception Undermine the World Trading System?* IEP@Bocconi Commentaries, No. 10 (25 January 2024). Available at: https://iep.unibocconi.eu/publications/will-national-security-exception-undermine-world-trading-system (Accessed: 30 October 2025).

tariffs are necessary for the long-term sustainability of the domestic steel and aluminum industries, which are, in turn, crucial for the national defense industry. The national security exception in Article XXI of the GATT has also been implicated in recent WTO disputes.[4] Legal arguments used when discussing the legitimacy of the US tariffs against China have included that the WTO does not have the competence to rule on the validity of the national security exception because it touches the core of a country's sovereignty. The right to depart from WTO rules for national security purposes is well-established safety valve in the WTO agreements, but ruling on its merits has been historically challenging. Since the invoking state is sovereign to decide if a particular trade situation forms a national security threat, how can the WTO intervene in the nation's domestic affairs to determine the notion of "national security"? This is a particularly prevalent question, also because it relates to questions surrounding digital protectionism; in fact, several digital protectionist measures are introduced under the premise that sensitive technological assets, trade secrets, and data must be protected, inter alia, for national security purposes.

1.2.Defining Digital Protectionism

Digital protectionism generally refers to the adoption of regulatory or policy measures that restrict, reshape, or condition participation in the digital economy with the aim of favoring domestic players. Unlike classical protectionism discussed above, which relies on tariffs, quotas, and

[4] World Trade Organization (WTO) (n.d.) *WTO Analytical Index, GATT 1994 – Article XXI (DS Reports), p. 3.* Available at: https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art21_jur.pdf (Accessed: 21 October 2025).

subsidies, digital protectionism tends to operate through *non-tariff barriers*, particularly rules around data, market access, and security. These measures may be motivated by diverse objectives: safeguarding individual rights (privacy), securing national infrastructure, ensuring economic competitiveness, or addressing power asymmetries in digital markets.

This distinguishes digital protectionism compared to traditional protectionism in that, unlike tariffs, subsidies and quotas which are easily detectable, digital protectionism relates to content moderation requirements, privacy rules, trade secrets protection, export restrictions on advanced semiconductors, and broader restrictions on cross-border data flows. This new era of protectionism, irrespective of its legitimacy and whether it is based on reasonable legal grounds, is markedly more difficult to trace.[5]

Although the objective of traditional protectionism is straightforward, i.e. to give domestic producers a competitive advantage, either by raising the costs of foreign goods or by lowering costs for local firms, the objective of digital protectionism is less obvious. The EU's narrative is primarily focused on human rights and respect of fundamental rights through safeguarding the right to privacy, while the US focuses more on national security, innovation and commercial initiatives. Exploring each angle can provide a legitimate argument for introducing digital protectionism, however, the EU and the US do not consider this as protectionism *per se*.

[5] Burri, M. (2017) 'The Regulation of Data Flows Through Trade Agreements', *Georgetown Journal of International Law*, 48 (1), pp. [408-448]. Available at: https://ssrn.com/abstract=3028137 (Accessed: 1 November 2025).

If anything, digital protectionism has provided new tools for the economy; rather than tariffs or quotas, states rely on non-tariff, regulatory, and infrastructural measures that govern data flows, digital platforms, and technology infrastructures.

Key instruments of digital protectionism include:

- **Data Localization Requirements**. The data localization requirements oblige companies to store or process personal data within a specific jurisdiction. In practice, such requirements benefit primarily domestic cloud providers since they become an essential component of the economy. Conversely, these requirements harm foreign providers, who need to either invest heavily on ground operations, or exit the market altogether. Governments justify localization on the basis of ensuring law enforcement access, enhancing cybersecurity, protecting privacy, or fostering domestic digital industries. In the EU, while the GDPR does not require localization, certain sectoral laws (e.g. in finance, health) have localization components. The US does not mandate data localization; rather, it resists it in trade negotiations, pushing for free flow of data with trust, a concept coined in 2019 to frame the international policy drive to promote the use of data for economic and social prosperity. According to the OECD, Japan introduced the "free flow of data with trust" concept at the World Economic Forum Annual Meeting in Davos in 2019, and in 2023 G7 leaders endorsed the concept's mission and priorities.[6] Localization overall directly benefits domestic providers and can operate as a protectionist measure, raising costs for global cloud and digital service firms.

[6] Organisation for Economic Co-operation and Development (OECD) (n.d.) *Data free flow with trust*. Available at: https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html (Accessed: 21 October 2025).

- **Restrictions on Cross-Border Data Transfers.** The EU's adequacy framework under the GDPR conditions data flows on the receiving country meeting "equivalent" privacy protections. The EU has approved a limited number of countries which provide equivalent protection to personal data. By creating a list of privileged countries that are "adequate", the EU by default excludes most of the countries globally.[7] The invalidation of the EU-US Safe Harbor (Schrems I) and Privacy Shield (Schrems II) agreements restricted transfers until the EU-US Data Privacy Framework. Although the EU-US Data Privacy Framework is considered an adequacy decision, it only applies to companies that self-certify to the framework, meaning that it does not automatically apply to the EU-US data transfers. For instance, if a company in the EU wants to transfer personal data to Argentina, it can do so without any restrictions. However, if the same company wants to transfer personal data to the US, it will need to rely on the recipient's Data Privacy Framework (DPF) certification since there is no blanket adequacy protection. If the recipient is not DPF certified, the company will need to rely on one of the remaining data transfer tools, as it would have done in any other third country.[8] The predominant data transfer tool used in such cases are the Standard Contractual Clauses (SCCs), which is a boilerplate contract pre-approved by

[7] Currently, the list includes the following countries: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organizations participating in the EU-US Data Privacy Framework), and Uruguay.

[8] Mattoo, A. and Meltzer, J. (2018) International Data Flows and Privacy: The Conflict and Its Resolution. World Bank Policy Research Working Paper. Washington, DC: World Bank.

the European Commission. The SCCs need to be executed between the relevant parties (the data exporter and the data importer) and include different modules depending on the data transfer reality (controller-controller, controller-processor, processor-processor, processor-controller). Since the SCCs cannot be modified between the parties, they impose a de fact burden on the data importer. This burden is considered necessary to adequately protect European personal data, however the SCCs impose various contractual requirements that include the appointment of subprocessors, data access and data use, and more. The US law does not generally impose adequacy conditions on outgoing flows, however data flows may be subject to additional scrutiny based on relevant Executive Orders, as further discussed below.

- **Platform Regulation and Competitions Rules**. The EU's Digital Markets Act (DMA) imposes strict obligations on "gatekeeper" platforms, the majority of which are large US technology companies. While this is framed as a broader competition law/antitrust measure, the footprint of the regulation overwhelmingly covers US tech companies. This resembles a chicken or the egg type of dilemma- one the one hand it is intuitive that the majority of the largest digital platforms regulated under the DMA are based in the US because the US is home to the largest tech companies; at the same time, a regulation explicitly targeting the major tech companies is, by default, US-centric since it is a well-established fact that the largest technology companies are based in the United States. In the US, enforcement under the FTC and DOJ has focused on antitrust lawsuits against domestic big technology companies, with less emphasis on foreign firms. Market-access restrictions are generally more likely to appear in sectoral laws (e.g. telecom procurement

bans). Similarly, the Digital Services Act creates obligations for online intermediaries and very large platforms regarding content moderation, transparency, and risk assessment.

- **Export controls and investment screening.** Export controls and investment screening are well-established tools that every country deploys to ensure that it protects valuable assets, and scrutinizes its investments. The US is increasingly using these tools to, practically, limit the transfer of advanced technologies (semiconductors, AI chips, quantum computing) to rival economies. This type of measures is typically justified on national-security grounds but also serves to entrench US leadership in strategic sectors. For instance, in October 2022 the US Commerce Department blocked advanced chip exports and related design software.[9] The rules implemented impose restrictive export controls on certain advanced computing semiconductor chips, transactions for supercomputer end-uses, and transactions involving certain entities. Also, the rules impose new controls on certain semiconductor manufacturing items and on transactions for certain integrated circuit (IC) end uses. Further, the US CFIUS (Committee on Foreign Investment in the United States) enjoys expanded jurisdiction to scrutinize foreign investments in critical technology. The EU framework on screening investments in critical technologies focuses more on 5G, cloud computing and AI.

[9] Bureau of Industry and Security, U.S. Department of Commerce (2022) Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC). Available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file (Accessed: 21 October 2025).

- **Industrial subsidies in technology.** Both the EU (e.g. with the European Chips Act)[10] and the US (e.g. CHIPS and Science Act)[11] are funneling public funds into domestic semiconductor production. Subsidies generally fall within traditional protectionism, however their application in digital sectors underscores the mix between old and new protectionist methods. Overall, industrial subsidies reinforce the issue of industrial policy, yet in a modern form.

On balance, the EU is generally more active in restricting cross-border data flows and platform regulation, whereas the US is focusing more on export controls and investment scrutiny. Both traditional and digital protectionism restrict market openness in ways that benefit domestic actors. They create compliance costs or outright barriers for foreign competitors. However, they have striking differences: (1) the visibility of traditional protectionist measures (tariffs, quotas) is such that they are transparent and easily quantifiable. Digital protectionism on the other hand is embedded in complex regulations and is difficult to detect; (2) traditional measures were founded in exclusively economic arguments, whereas digital measures are usually weaved into broader considerations including human rights, security, or sovereignty; (3) the scope of the measures

[10] European Union (2023) Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (Text with EEA relevance). Official Journal of the European Union, L 229, 18.9.2023.

[11] United States Congress (2022) Public Law No. 117-167. CHIPS and Science Act of 2022. Washington, DC: U.S. Government Publishing Office.

varies since traditional protectionism spans all sectors, as data and digital infrastructures underpin nearly every industry; and (4) the international legal discipline covering these measures varies: WTO law is a well-established source that regulates tariffs and quotas but has generally weaker and more contested rules for digital measures. Whenever states have a trade dispute, the WTO is the natural redress mechanism -notwithstanding the Appellate Body's paralysis since 2019.[12] However, when it comes to digital protectionism, it is unclear how it will be regulated, what is the available redress mechanism, and what course of action the affected stakeholders have.

Overall, the shift from traditional to digital protectionism complicates the regulatory and trade landscape. Digital measures serve multiple objectives, and it is more difficult to label them as protectionist. Moreover, since the digital economy is transnational, measures with legitimate public-interest rationales can produce significant protectionist spillovers.

2. Digital Protectionism Manifestation in the EU

2.1.Manifestations in the European Union

[12] "World Trade Organization (2019) 'Members reiterate joint call to launch selection process for Appellate Body members.' World Trade Organization News, 22 November. Available at: https://www.wto.org/english/news_e/news19_e/dsb_22nov19_e.htm (Accessed: 21 October 2025).

In the EU, digital protectionism often takes a rights-based and sovereignty-driven form. For instance:

- **Data protection and privacy regulation**: The GDPR exemplifies the EU's emphasis on data as a matter of fundamental rights. The regulation is not proactively protectionist, however it includes extraterritorial provisions that impose significant compliance obligations, and consequently introduce costs to businesses. The extraterritorial application of the law also creates a domino effect whereby businesses need to invest heavily in order to comply with the respective data privacy provisions. Most companies which are not established in the EU/UK need to take into consideration issues of data flows, in particular pursuant to the Schrems I[13] and Schrems II[14] rulings of the Court of Justice of the EU, as well as issues of broader compliance including maintaining records of processing activities, data processing agreements, data subject requests agreements, data retention schedules, information security policies, and related compliance items (Bradford, 2020).[15]
- **Digital sovereignty initiatives**: The EU has framed digital regulation within the context of sovereignty and "strategic autonomy", a concept which the EU has set up in the decade

[13] Court of Justice of the European Union (CJEU) (2015) Case C-362/14, Judgment of the Court (Grand Chamber). Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650.

[14] Court of Justice of the European Union (CJEU) (2020) Case C-311/18, Judgment of the Court (Grand Chamber). Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. ECLI:EU:C:2020:559.

[15] Bradford, A. (2020) The Brussels Effect: How the European Union Rules the World. Oxford: Oxford University Press.

2013-2023.[16] Relevant laws include the Digital Markets Act (DMA) and the Digital Services Act (DSA), which explicitly target large platforms, introducing obligations on competition, transparency, and content moderation. Other laws that have been recently implemented include the EU AI Act and the EU Data Act, which extend the regulatory scope by regulating emerging technologies and ensuring EU control over data infrastructures.

2.2.Applying the framework: the GDPR

The GDPR has arguably been the crown jewel of the EU regulatory landscape since 2018. It modernized the protection of personal data in Europe, and has significantly influenced many jurisdictions globally. It is the epitome of the EU's soft power, largely due to its status as a large economy. Under the GDPR, the protection of privacy and personal data is routed in human rights protection, since privacy is being treated as a fundamental right. This is consistent with the EU Charter of Fundamental Rights, while the EU privacy standards become a de facto global baseline (in particular, Article 8- Protection of personal data of the EU Charter is relevant).

An argument can be made, however, that the GPDR introduces digital protectionism, for instance through the introduction of adequacy decisions that provide a list of "adequate" countries, hence by default excluding any country not on that list. The limited number of third countries also

[16] European Parliamentary Research Service (EPRS) (2022) EU Strategic Autonomy 2013–2023: From Concept to Capacity. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589 (Accessed: 21 October 2025).

showcases that the EU only considers a handful of jurisdictions as adequate, and generally treats the majority of the jurisdictions as non-equal. This makes cross-border data flows challenging, and often leads companies to invest in domestic data centers to avoid falling afoul of the GDPR.

For instance, the Schrems II ruling could qualify as digital protectionism to the extent that it invalidated a data transfer mechanism (the Privacy Shield in 2020) while it had also invalidated another data transfer mechanism a while ago (the Safe Harbor in 2015). In particular, the European Court of Justice (ECJ) declared the EU-US Privacy Shield framework invalid on 16 July 2020. In its ruling, the ECJ upheld the EU Standard Contractual Clauses (SCCs) but confirmed that the companies must verify prior to any transfer using SCC that the parties can effectively provide the level of protection required by EU law.[17] The ECJ ultimately invalidated the Privacy Shield on two grounds: (i) it does not offer adequate protection to individuals' data protection rights in light of the broad disclosure of personal data to the US intelligence services; and (ii) the Ombudsperson included in the Privacy Shield framework was not practically effective and did not address complaints received by EU citizens, also contributing to an overall lack of independence and authority to adopt decisions that are binding on US intelligence services.

In particular, the ECJ ruled that U.S. domestic law does not offer a standard of legal protection that is "essentially equivalent" to the standard of protection under EU law. The ECJ found that national intelligence programs authorized by Section 702 of the Foreign Intelligence Surveillance

[17] For a more detailed discussion about the Safe Harbor and the Privacy Shield, see Nikolaos I. Theodorakis, EU-US Data Transfers in the Aftermath of the Privacy Shield Invalidation, Stanford-Vienna TTLF Working Paper No. 80, http://ttlf.stanford.edu.

Act (FISA) and Executive Order 12333 do not grant EU individuals actionable rights before the courts against U.S. authorities, rendering the data protection rights insufficient. Kuner (2020) stresses that adequacy is not framed as protectionism, but its effect is to privilege those countries aligned with EU standards. This rights-based orientation makes the EU an outlier: where the US frames privacy as a consumer-protection issue, the EU treats it as a constitutional guarantee.

The ECJ noted that the Charter of Fundamental Rights of the European Union (Charter) protects individuals' private communications and personal data. Disclosing data to a third party—including public authorities—interferes with these rights, and is permitted only if strictly necessary.[18]

However, the ECJ indicated that surveillance programs like Presidential Policy Directive-28 regarding signals intelligence activities may process a disproportionate amount of data and allow access to data in transit to the U.S. without any judicial review. The ECJ reasoned that the surveillance programs are not limited in scope and do not provide guarantees for potentially targeted non-U.S. individuals. As such, individuals do not have an effective judicial remedy to exercise their privacy rights.[19]

2.3. Digital Markets Act / Digital Services Act

[18] *Ibid*

[19] Court of Justice of the European Union (CJEU) (2020) Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. ECLI:EU:C:2020:559, paras 56 et seq.

During 2020, the European Commission published a set of proposals geared to, inter alia, regulate digital platforms. The relevant package included the Digital Markets Acts (DMA), addressing primarily antitrust-related requirements, and the Digital Services Act (DSA), addressing primarily regulatory matters. The DMA/DSA package is added to a new ecosystem that is being created to complement the General Data Protection Regulation (GDPR) and regulate online service providers as long as they target EU consumers. Companies subject to the DSA/DMA include several US companies, making this a matter of interest on both sides of the Atlantic. Apart from the DMA and the DSA, European institutions are now in the process of drafting/finalizing two more initiatives, the AI Act and the Data Act. Once finalized, these four new acts will create a new regulatory landscape that companies will need to comply with depending on the nature and scope of their services.

In particular, the DSA attempts to regulate long-debated topics such as: (i) the liability of online platforms; (ii) the platforms' obligations regarding content moderation and (iii) advertising transparency to avoid user manipulation. The DSA/DMA apply to digital services, subject to scoping conditions, including social media, online marketplaces and other online platforms. As such, EU companies and US companies active in the EU will need to consider how these rules may affect their operations and the respective obligations they may have. The paper will discuss the history behind the DSA/DMA proposal.

The DSA introduces a legal framework for content, products, and services offered by intermediary services providers. It steps up the compliance requirements since it creates new obligations for all intermediary service providers, including online platforms. The regulatory burden imposed by the

DSA overall varies depending on the type of services offered. In its first significant draft of December 2020, the DSA followed a layered approach with building blocks of obligations, depending on the size and function of an intermediary service. The DSA in particular covers four types of service providers: (1) intermediary services, including "mere conduit" and "caching" services; (2) hosting services (e.g. cloud and web hosting services); (3) online platforms (e.g. online marketplaces, app stores, and social media platforms); and (4) "very large" online platforms, which are defined as platforms reaching more than 10 percent of the then current EU population, currently estimated at 45 million users. Since the DSA obligations are working in building blocks, the more data heavy a company is, the more steps it will need to take to comply, while having complied with all the previous steps.[20]

The Digital Services Act largely builds on the Commission Recommendation 2018/314, which had signaled that a relevant EU regulatory initiative was in the works, at the same year when the GDPR entered into force in the EU, another landmark legislation for the EU. The European Commission launched a public consultation to gather evidence in the course of 2020. The European Commission also published an impact assessment, which is customary for this type of legislative acts. The DSA is aimed at enhancing content moderation on social media platforms, pursuant to increasing calls regarding illegal content. Key innovations of the DSA include new obligations on intermediaries, content moderation obligations, and the cooperation and enforcement between the European Commission and national authorities. The DSA is inheriting

[20] For a more detailed discussion about the Safe Harbor and the Privacy Shield, see Nikolaos I. Theodorakis & Dimitra Tzeferakou, The EU-US Data Privacy Framework: A new path for transatlantic data transfers?, TTLF Working Papers No. 109, Stanford-Vienna Transatlantic Technology Law Forum (2023).

the e-Commerce Directive's provisions regarding liability, meaning that companies which host other's data, and intermediaries are not liable for the content of the information they host, unless they have actual knowledge that the content is illegal, or if they do not act in accordance with the law once they are alerted to the fact that they host illegal content. This notion is known as "conditional liability exemption", meaning that intermediaries and hosting services are not always exonerated from liability, but rather under specific conditions.

The DSA is structured in a layered manner, meaning that the most detailed obligations only apply to platforms with a significant number of users in the European Union (i.e. more than 45 million users). However, even smaller platforms will have obligations, it is just that they will not be as onerous/detailed as the requirements prescribed to large platforms. The building block approach is therefore a proportionate way to avoid "one-size-fits-all" compliance, but rather to comply in accordance with the actual strength/size of the company's presence in the EU. It is noteworthy that European policymakers felt a greater sense of urgency to move the legislation forward in a call to ensure that major tech platforms were transparent and properly regulated. The DMA and DSA fit in the broader European Digital Strategy announced by the European Commission. The Commission's intention was primarily to review the rules applicable to digital platforms and propose a new framework that ultimately aims to booster the single market for data and ensure Europe's global competitiveness. These initiatives, taken together, want to ensure that data can flow in accordance with the principles of competition law and data protection. The DMA therefore outlines a new enforcement framework, whereas the DSA regulates the liability of platforms and imposes new obligations with respect to content moderation, due diligence of illegal content, and transparency of advertising.

An argument has been made that the DSA and the DMA disproportionately affect non-EU Big Tech (mostly US firms). While the primary purpose is competition/consumer-protection related, the enforcement costs and compliance reshape competitive dynamics to an EU advantage. The rules are formally neutral, yet the measures disproportionately affect US tech giants, whereas EU-based competitors benefit from levelling measures. The EU does not consider its measures as protectionist, but rather argues that they are measures that pursue legitimate measures, and promote universalizable goals. Yet, critics such as the US would typically view these measures as disproportionately targeting foreign firms, and introducing barriers to trade.

3. Digital Protectionism Manifestations in the United States

The US has traditionally resisted characterizing its measures as protectionist, emphasizing free markets and innovation. The US approaches digital governance from a different mix of institutional, legal, and political rationale than the EU. Historically committed to market openness and innovation, US policy has nonetheless developed a distinct set of instruments that—while framed in terms of national security, economic competitiveness, and innovation policy—can have protectionist effects. The US toolkit is less centralized (i.e. it does not deploy centralized measures such as the GDPR), and relies more on targeted intervention. This includes export controls, investment screening, industrial subsidies, and tailored state-level privacy regimes.

- **Export controls and investment screening**: The US introduces restrictions on exports of advanced semiconductors, AI technologies, and quantum computing. Rather than a blanket

prohibition, the US is focusing more on countries like China.[21] The Committee on Foreign Investment in the United States (CFIUS) scrutinizes foreign acquisitions in sensitive tech sectors for purposes of national security. The measures are designed to shield domestic industries from foreign competition, in an effort to control how critical commodities are traded among countries.

- **Privacy regulation at the state level**: The US does not have a federal equivalent to the GDPR, however several states have introduced their own data protection laws. These include the California Consumer Privacy Act (CCPA) and its amendments (CPRA), as well as states such as the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA). The US privacy landscape is overall less restrictive than the GPDR, and more fragmented altogether, but it still introduces some obligations that companies operating in the US need to comply with from a privacy standpoint.
- **Industrial policy**: Industrial policy is not a practice of the past; in fact, every country nowadays is using industrial policy as a tool and a mechanism to achieve its goals. The US, like many other countries, has committed substantial subsidies to domestic technology industries: for instance the US CHIPS Act includes $39 billion in subsidies for chip manufacturing on US soil along with 25% investment tax credits for costs of manufacturing

[21] Egmont Institute (2023) Hall of Mirrors: How US-China Export Controls Feed Each Other. Available at: https://www.egmontinstitute.be/hall-of-mirrors-how-u-s-china-export-controls-feed-each-other/ (Accessed: 21 October 2025).

equipment, and $13 billion for semiconductor research and workforce training.[22] These initiatives are geared to reduce reliance on foreign supply chains and gain traction in sectors of importance.[23]

3.1. Export controls & CFIUS

Export controls and CFIUS are two key components of the U.S. national security architecture that relates to cross-border flows of goods, technology, and capital. The Export Administration Regulations (EAR[24] administers export controls, and the International Traffic in Arms Regulations (ITAR)[25] attempts to prevent the transfer of sensitive technologies, dual-use items, and defense-related materials. In an intensifying geopolitical competition, especially between the United States

[22] Semiconductor Industry Association (SIA) (2023) America's Chip Resurgence: Over $630 Billion in Semiconductor Supply Chain Investments. Available at: https://www.semiconductors.org/chip-supply-chain-investments/ (Accessed: 21 October 2025).

[23] Aaronson, S.A. (2018) 'Data is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows', Digital Policy, Regulation and Governance, 20(6), pp. 479–493.

[24] Bureau of Industry and Security, U.S. Department of Commerce (n.d.) Export Administration Regulations (EAR). Available at: https://www.bis.gov/regulations/ear (Accessed: 1 November 2025).

[25] U.S. Department of State, Directorate of Defense Trade Controls (n.d.) International Traffic in Arms Regulations (ITAR). Available at: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987#sideNav (Accessed: 1 November 2025).

and China, export controls have unfolded into a tool of economic statecraft. CFIUS supplements the export control regime, and scrutinizes Foreign Direct Investment (FDI) in U.S. companies and assets that assess potential risks to national security. It is enshrined with wide powers to review, modify or block transactions regarding foreign persons acquiring control. The Foreign Investment Risk Review Modernization Act (FIRRMA) further expanded CFIUS's jurisdiction to include non-controlling investments and avenues for technology transfer.

Export controls and CFIUS form a dual-layered framework that governs the interface between national security and global economic integration. Yet, these mechanisms raise complex legal and policy questions regarding transparency, due process, and broader issues of legitimate trade and innovation. As global supply chains become increasingly interdependent, the coordination between export control enforcement and foreign investment review will define the evolving landscape of US economic security governance.

Export controls overall aim to prevent the unauthorized transfer of strategic and dual-use technologies that could empower or enhance the military or intelligence capabilities of other countries. These processes are designed with a view of creating an adequate buffer of export controls, primarily administered by the Bureau of Industry and Security (BIS) under the Department of Commerce through the Export Administration Regulations (EAR), and by the Directorate of Defense Trade Controls (DDTC) under the Department of State through the International Traffic in Arms Regulations (ITAR). The regimes cover a wide range of items, from semiconductors to encryption software and artificial intelligence systems. They are also increasingly used as tools of strategic competition and foreign policy leverage. Recent initiatives

include the U.S. Export Control Reform Act of 2018[26] and the coordinated restrictions on semiconductor exports in China. They overall reflect a shift from transactional control mechanisms to frameworks designed to safeguard global supply chains.

CFIUS operates under the authority of Section 721 of the Defense Production Act of 1950. It was, however, reformed significantly by the FIRRMA of 2018, enabling it to function as a multi-agency committee tasked with reviewing foreign investment transactions that could result in control, or even partial influence, over US companies that are imperative to national security. For instance, depending on the US state law that applies, such control threshold may be less than a majority shareholding in a company. The company's jurisdiction often extends to sectors that involve critical technologies, critical infrastructure, and sensitive personal data. This scope of application reflects a growing recognition that national security risks extend beyond traditional defense assets to encompass data-driven platforms and emerging technologies. In practice, CFIUS often operates as an essential gatekeeper for cross-border investment, which may also recommend divestment as or when necessary.

Taken together, export controls and CFIUS form a comprehensive system to manage the interplay between open markets and national security. It is a challenge to do so in a globalized economy, yet their convergence highlights the increasing complexity of regulating intangible assets such as data, intellectual property, and know-how. These resources are strategically valuable as physical commodities, but the framework's interpretation presents significant challenges. For instance, it

[26] United States Congress (2018) Export Control Reform Act of 2018, H.R. 5040, 115th Congress. Available at: https://www.congress.gov/bill/115th-congress/house-bill/5040 (Accessed: 13 November 2025).

may lead to an overly expansive application of export controls and investment screening risks, create an impediment to collaborate in global research networks, and act as an invitation to retaliatory measures from other jurisdictions.

This is not to say that under-regulation is the best way forward; in fact, it would allow adversaries to take advantage of the regulatory loopholes and acquire cutting-edge technologies and know how. Economic policy and security strategy often intertwine, and it is challenging to determine which takes priority, and which is leading the race. These blurred lines mean that effective governance will depend on maintaining transparency, predictability, and international coordination. It also means that export controls and CFIUS embody both tensions and necessities with respect to technological sovereignty in an era of strategic interdependence.

3.2. Privacy Regulations

Unlike the EU's single, comprehensive federal regulation, the US has developed a heterogeneous landscape of privacy rules, with leading states such as California (CCPA/CPRA),[27] Virginia (CDPA),[28] and Colorado[29] adopting comprehensive privacy statutes. Ultimately, these rules lead

[27] California Office of the Attorney General (n.d.) California Consumer Privacy Act (CCPA). Available at: https://oag.ca.gov/privacy/ccpa (Accessed: 13 November 2025).

[28] Virginia General Assembly (n.d.) Code of Virginia, Title 59.1, Chapter 53. Available at: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (Accessed: 13 November 2025).

[29] Colorado Office of the Attorney General (n.d.) Colorado Privacy Act. Available at: https://coag.gov/resources/colorado-privacy-act/ (Accessed: 13 November 2025).

to a fragmented compliance environment, since companies are uncertain with respect to the compliance expectations based on their presence and clientele. Diverging obligations can also lead to situations of conflict of laws, where companies face contradictory obligations in the US vs. the EU. As a result, several companies end up complying with all the state privacy laws and the GDPR, adopting a belt and suspenders compliance strategy.

3.3. Industrial subsidies (CHIPS Act, state aid-like measures)

Industrial subsidies—government measures designed to support strategic sectors through financial incentives, tax breaks, or direct investment—have re-emerged as central tools of economic and technological policy in advanced economies. The US CHIPS and Science Act of 2022[30] represents a major legislative shift to endorse domestic semiconductor manufacturing. It also aims to strengthen supply chain resilience, and reduce dependency on foreign networks. In doing so, the CHIPS Act allocates approximately $52 billion in federal subsidies, grants, and tax incentives to encourage private sector investment in semiconductor fabrication, research, and workforce development. Beyond the immediate economic rationale, the CHIPS Act reflects a broader geopolitical concern: the desire to maintain US leadership in critical technologies that underpin artificial intelligence and defense systems, while countering industrial policies of competitors such as China. In this respect, industrial subsidies have shifted from being viewed primarily as market distortions to being understood as instruments of national security and strategic autonomy. Unlike

[30] United States Congress (2021) H.R. 4346, 117th Congress. Available at: https://www.congress.gov/bill/117th-congress/house-bill/4346 (Accessed: 13 November 2025).

EU sovereignty rhetoric, US industrial policy is animated by a bipartisan consensus that supply-chain fragility is a national-security vulnerability. The result is a large-scale re-shoring effort.

The US has deployed targeted bans and procurement restrictions against specific foreign vendors on grounds of national security. Other countries have also followed suit. The Federal Acquisition Regulation and sectoral rules often exclude vendors deemed risky from government contracts, granting preferential market access to domestic or allied suppliers in sensitive procurements. These measures reshape market opportunities in critical infrastructure, effectively favoring certain suppliers while excluding others on legitimate security grounds but with clear protectionist side effects.

The CHIPS Act also signals a normative and structural transformation in U.S. economic governance, traditionally skeptical of "state intervention" compared to European or East Asian models. Historically, U.S. industrial policy operated indirectly through defense spending, research grants, or tax incentives rather than overt subsidies. However, the convergence of supply chain disruptions during the COVID-19 pandemic, rising U.S.–China tensions, and the recognition of semiconductor vulnerabilities has led to a recalibration of this stance. The Act's approach, combining subsidies with regulatory conditions such as prohibitions on expanding production in China, mirrors, in practice if not in law, the "state aid" mechanisms long employed by the European Union to direct industrial transformation under public oversight. This convergence suggests an emerging global consensus that targeted state support can be compatible with open market principles when justified by strategic and security concerns. Yet it also raises complex legal

questions regarding compliance with World Trade Organization (WTO) rules and the potential for subsidy races that could distort international competition.

At the same time, the CHIPS Act and similar state aid-like measures highlight a growing tension between national industrial policy and the norms of global economic governance. While these subsidies aim to enhance resilience and technological sovereignty, they risk fragmenting global value chains and reinforcing techno-economic blocs. For instance, the European Union's own response, through its European Chips Act and relaxed state aid rules, illustrates the domino effect as allies seek to avoid strategic dependency while preserving competitiveness. Moreover, the turn to industrial subsidies invites debate about efficiency, accountability, and distributional equity: whether public funds allocated to large corporations yield broad-based societal benefits or merely entrench private monopolies. From an academic perspective, these developments mark the return of the "developmental state" paradigm within advanced capitalist economies, albeit reconfigured for the twenty-first century's geopolitical and technological context.[31] Based on the above, industrial policy is more relevant than ever. Governments pivot to a form of digital protectionism, deploying industrial policies in a digital era and crafting industrial policy frameworks that enhance innovation and security. The policy frameworks are geared to enhance innovation and security, while maintaining the legitimacy of the global trade regime, and the rules of fair competition.

[31] Nem Singh, J. & Ovadia, J.S. (2018) 'The theory and practice of building developmental states in the Global South', Third World Quarterly, 39(6), pp. 1033-1055. Available at: https://doi.org/10.1080/01436597.2018.1455143 (Accessed: 13 November 2025)

The CHIPS Act overall illustrates a broader evolution in US industrial policy, which has historically favored market-led development and indirect forms of support, including federal research grants and defense procurement. The CHIPS Act represents a more interventionist approach, providing incentives to private investment along with regulatory conditions, such as restrictions on expanding production in China. The rationale behind this is to align private sector behavior with national security objectives. The CHIPS Act is structured in a similar way as the EU's state aid mechanisms, which largely allow EU member states to provide subsidies under controller conditions. This contrasts with the general rule of thumb, which is that subsidies and state aid are illegal under the WTO rules. Both frameworks showcase a policy shift; advanced economies increasingly recognize that selective state support can be compatible with open markets when strategic priorities justify this. However, this begs the questions of WTO compliance, particularly since the WTO has introduced several agreements prohibiting subsidies, and in general subsidies are considered harmful for the economy, market distorting, and an inefficient way to advance a country's own interests.

Similarly to subsidies, industrial policies highlight the controversy between domestic policy objectives and global economic governance. Measures such as the CHIPS Act are well intended, and designed to enhance technological resilience and national security, they can fragment global value chains, and endorse protectionism. In fact, the very notion of industrial policy is a protectionist concept, meaning that any form of such policy advances protectionism over liberalism. Apart from the geopolitical concerns that are prevalent, industrial subsidies create issues of economic efficiency, as well as broader questions of international development and growth. The challenge lies in designing subsidy frameworks that foster innovation, enhance

resilience, and secure strategic autonomy without undermining fair competition, global trade norms, or long-term economic sustainability.

The US approach is overall instrumentally selective, deploying legitimate policy tools (security, investment screening, subsidies) that may have protectionist side effects. Industrial subsidies and export controls are openly economic and can be seen as protectionist by design; investment screening and procurement exclusions are security measures with protectionist impacts; state-level privacy laws impose compliance costs that indirectly affect foreign firms. Unlike the EU, which uses rights-based ex ante regulation to project normative standards globally, the US tends to rely on narrow, strategic, and often bilateral or plurilateral measures that aim to shape technological competition while minimizing multilateral rule-making. That strategy achieves targeted protection of domestic capabilities but risks reactive fragmentation when other powers (EU, China, India) adopt their own defensive or sovereignty-based regimes.

The US model of digital protectionism is therefore a hybrid: less rhetorical emphasis on sovereignty and fundamental rights than the EU, but more assertive use of industrial, security, and investment instruments to shape the digital order.

4. EU-US Comparative Perspectives

4.1. Diverging paths…

At a high-level, the EU and the US anchor digital policy in different legal and perceptual traditions. The EU treats data protection and privacy as a fundamental right, and pursues comprehensive rules regarding extraterritorial reach, and a suite of recent sectoral laws that directly regulate platform powers. These instruments are crafted with privacy by design in mind, along with ensuring market fairness and pursuing digital sovereignty. The EU is using its soft power by exporting standards to stay compliant with the EU market, which is one of the largest markets globally. This "Brussels Effect" regulates how companies can enter the European market, while remaining in compliance with regulatory requirements. [32]

By contrast, the US mixes a normative preference for market openness with targeted strategic instruments. Rather than a single sweeping privacy regime, the US deploys a patchwork of state laws (e.g. CCPA/CPRA) and relies heavily on instruments frames as national-security or competitiveness tools, including export controls, investment screening (CFIUS), and industrial subsidies (CHIPS Act). These measures are generally more targeted, even surgical, than the EU ex ante rules that apply holistically, but can produce equally significant effects on market access and technology diffusion.

The instruments each side favors generally create different kinds of frictions. EU regulation tends to be rule-based and universal, as it applies obligations by function rather than nationality. Since the largest platforms and data controllers/processors are US-headquartered, compliance burdens fall heavily on US firms, producing practical protectionist effects even where the legal text is

[32] Bradford, A. (2020) The Brussels Effect: How the European Union Rules the World. Oxford: Oxford University Press.

neutral. The EU is therefore largely exporting its regulation and adopting an extra-territorial reach. The US toolkit often targets geopolitical rivals, and introduces nuanced measures to prevent or reduce technology transfer. For instance, the CHIPS Act ties funding to onshore production and restricts recipients' overseas expansion in certain geographies.

The diverging paths between the EU and the US risk fragmenting the global digital economy since companies will be subject to multilayered compliance, and can possibly face conflicting requirements. For instance, different regulations in the EU and the US may require a company to ensure that its data cannot be accessed by any foreign authorities, while at the same time that it must make such data available on request. The multi-layered approach adds to the compliance costs of companies, and creates uncertainty.

Further, divergence between the EU and the US leaves space for other models to gain traction. Examples include China's model which is more state-centric, as well as India's protectionist posture on data which favors consent and data localization. The plethora of issues pertinent to data localization, and more broadly to GATS, will lead to several disputes before the WTO when adjudicating trade differences, particularly given the existing Appellate Body deadlock.

4.2. Or Converging Paths?

Despite the differences mentioned above, the EU and the US are converging in areas of security, supply chains, and strategic autonomy. Both sides view certain digital assets (semiconductors,

cloud infrastructure, AI capabilities, 5G networks) as strategic. This is evident in the EU's Chips Act and the US CHIPS subsidies.

Institutionally, the EU-US Trade and Technology Council (TTC) and the negotiated EU-US Data Privacy Framework show both willingness and limits of coordination: as further explained below, the TTC creates workstreams to manage friction, an example being the DPF which restored an adequacy-based channel after Schrems II. These mechanisms demonstrate an appetite for cooperation even as deep legal and political divergences persist. These examples showcase that, notwithstanding the differences in approach regarding what digital protectionism has brought, it also creates the potential for strategic collaboration. While differences in legal culture and geopolitical strategy remain, the EU and the US recognize that digital policy, particularly in areas like privacy, AI and semiconductors, cannot be managed unilaterally without significant costs. The prospects for collaboration hinge on identifying shared objectives, designing interoperable standards, and balancing autonomy with cross-border integration.

Further, the EU and the US share a commitment to certain democratic principles, such as freedom of expression, consumer protection, and the prevention of monopolistic domination in digital markets. Coordinated approaches to transparency and risk mitigation could create mutually compatible rules for large global platforms, reducing compliance costs and friction.

4.3. The Future of the EU-US Digital Cooperation

The US and the EU are top trading partners, whereas their economic partnership has been instrumental to the growth and development of the digital economy. For instance, in 2019 alone the US exported $196 billion worth of information and communications technology (ICT) services to the EU.[33] Similarly, the EU is one of the wealthiest regions globally, and particularly attractive for US companies. The EU recently adopted "A New Transatlantic Agenda for Change", including a proposal for a US-EU tech and trade council to shape global tech standards and solutions.[34]

US and EU governmental bodies have proposed new bilateral efforts to address digital technology challenges. For instance, in December 2020, the European Commission and the EU's High Representative for Foreign Affairs and Security Policy issued a "new EU-US Agenda for Global Change" on the basis of the EU's common values, interests, and influence.[35] The tech agenda intends to create a "transatlantic technology space that can form the backbone of a wider coalition of like-minded democracies that have a shared vision on tech governance". The EU explicitly calls out cooperation on issues of AI, data flows, online platforms, competition, taxation in the digital economy, and standards.

[33] Fefer, R. F. (2021) EU Digital Policy and International Trade (CRS Report R46732). Congressional Research Service. Available at: https://www.everycrsreport.com/reports/R46732.html (Accessed: 1 November 2025).

[34] European Commission (2020) 'Commission welcomes the political agreement on the Digital Markets Act', Press-Release IP /20/2279. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279 (Accessed: 13 November 2025).

[35] *Ibid*

The EU-US Trade and Technology Council (TTC) was announced at the US-EU summit in June 2021 for the purpose of leading a "value-based digital transformation of Europe". The major goals for the TTC include reaching a common ground and strengthening global cooperation on technology, digital issues, and supply chains. The TTC also aspires to facilitate regulatory policy and enforcement cooperation. Key objectives of the partnership include: (i) ensuring that trade and technology serve the EU and US societies and economies; (ii) strengthening technological and industrial leadership; and (iii) expanding bilateral trade and investment.

On 5 December 2023, the TTC provided an update on several aspects of ongoing digital projects, including regarding online platforms. The US and the EU issued a first joint roadmap on the evaluation and measurement tools for trustworthy AI and risk management (AI Roadmap). The purpose of the roadmap is to inform the EU-US approach to AI risk management and trustworthy AI on both sides of the Atlantic. The EU and the US are also in the process of establishing an expert task force to reduce barriers to research and development collaboration on quantum information science and technology, develop frameworks for assessing technology readiness, discuss intellectual property, and export control-related issues, and work together on these international standards. In particular, the TTC confirmed that it plans to launch workstreams on Post-Quantum Encryption and Internet of Things (IoT), along with a preliminary focus on technical and performance standards for cybersecurity. The TTC also crafted the agreement on the principles of the Declaration for the Future of the Internet (DFI).[36]

[36] United States Trade Representative (USTR) (2022) 'U.S.-EU Joint Statement of the Trade and Technology Council', 5 December. Available at: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/us-eu-joint-statement-trade-and-technology-council (Accessed: 21 October 2025).

In terms of nexus points with next deliverables, the EU and the US can attempt to move towards mutual recognition and interoperable standards. By pursuing targeted mutual recognition in privacy (e.g. operationalizing adequacy with practical safeguards), cybersecurity certification, and AI risk assessment, the EU and the US can reduce duplicative compliance burdens while preserving core values.

The EU and the US can also create joint guidelines on export-control licensing, and allowable civilian collaboration so that security controls do not stifle benign scientific cooperation, while retaining necessary restrictions on dual-use items. For instance, the US Government Accountability Office and the Department of Commerce reports showcase the complexity but also the necessity of calibrated approaches. Further, the EU and the US can coordinate industrial policy with guardrails, align subsidy rules and procurement standards to avoid subsidy races, while cooperating on supply-chain resilience. For example, the CHIPS and the EU Chips Act demonstrate political appetite for such coordination.

Finally, the EU and the US can empower multilateral forums for digital trade and policy; the TTC can be used as a case study to broaden buy-in and prevent fragmentation. At the same time, international organizations like the WTO should be strengthened and relied on; the EU and the US can be driving forces, and can exercise significant power, in trying to resolve the Appellate Body deadlock which currently undermines the WTO's legitimacy.

5. Conclusion

Overall, digital protectionism is increasingly shaping the contours of the global digital economy. Both the European Union and the United States have adopted measures that, while justified through strategic or security rationales, produce outcomes that affect market access, innovation, and international trade. The measures may include a menu of options, such as data-related restrictions, platform regulation, export controls, investment screening, and targeted industrial subsidies. Taken together, they reveal a complex landscape in which legitimate regulatory goals and protectionist effects often intertwine.

The paper has overall sought to examine these dynamics without prejudicing their efficiency or legitimacy. Digital protectionism is used descriptively rather than normatively, capturing the ways in which both the EU and the US act to safeguard domestic markets, technologies, or values in the digital realm. The EU's mindset revolves around the notion of human rights, and how the protection of personal data, and individuals' privacy, is a rights-related issue. A culmination of legislation including the GDPR, the DMA, DSA, the AI Act, and the Data Act illustrate the EU's priorities, how they are enshrined in neo-industrial policy, and how the EU attempts to exercise its sphere of influence through the extraterritorial reach of its legislation. The US, on the other hand, uses a mix of national-security measures, export controls, and investment screening. Its privacy landscape is rather fragmented. Ultimately, both the EU and the US produce protectionist effects, but the angle is different in each case.

While we witnessed convergence in certain areas of shared strategic concern (e.g. supply chains, semiconductors, 5G), the EU and the US will likely continue to diverge in how they regulate digital services, and consequently how they impact the rise of digital protectionism. The EU is bound to continue enforcing its existing regulations, all of which have extraterritorial application. However, it is unlikely that the EU will introduce additional rules regarding the digital economy any time soon; the existing set of rules is already gathering significant criticism regarding red tape and bureaucracy, which therefore makes the region unattractive to businesses and investments. In fact, the EU has recently withdrawn some initiatives from its upcoming regulatory agenda, such as the AI Liability Directive and the Regulation on Standard Essential Patents, which would otherwise create additional compliance obligations for companies.[37] The US will also likely proceed with the security concerns and investment priorities that have been driving its measures in the past years.

Notwithstanding the above differences, which will likely persist in the coming years, the EU and the US countries have already collaborated in certain initiatives, such as the EU-US Data Privacy Framework and the TTC. This is a promising ground of cooperation so that the EU and the US pursue further collaboration in harmonizing standards, coordinating industrial policy, and strengthening global governance institutions such as the World Trade Organization.

Ultimately, the rise of digital protectionism largely reflects the broader tectonic changes that we experience in the global economy. Factors such as the increasing centrality of data, AI, and other

[37] Euronews (2025) 'EU Commission confirms ditching of AI liability and patents proposals', 31 July. Available at: https://www.euronews.com/next/2025/07/31/eu-commission-confirms-ditching-of-ai-liability-and-patents-proposals?utm_source=chatgpt.com (Accessed: 13 November 2025).

technologies contribute to the digital ecosystem, and potentially to digital protectionism. The trajectory of digital governance will overall depend on whether these two major powers can translate shared strategic interests into interoperable, coherent, and rules-based frameworks that preserve openness and autonomy.