Atlantic Council
EUROPE CENTER

Digital sovereignty: Europe's declaration of independence?

Frances Burwell, Kenneth Propp

Atlantic Council

The Europe Center

The Atlantic Council's Europe Center conducts research and uses real-time analysis to inform the actions and strategies of key transatlantic decision-makers in the face of great-power competition and a geopolitical rewiring of Europe. The center convenes US and European leaders to promote dialogue and make the case for the US-EU partnership as a key asset for the United States and Europe alike.

The center's Transatlantic Digital Marketplace Initiative seeks to foster greater US-EU understanding and collaboration on digital policy matters and makes recommendations for building cooperation and ameliorating differences in this fast-growing area of the transatlantic economy.

Authors

Frances Burwell

Kenneth Propp

Acknowledgments

The authors would like to thank James Batchik, Emma Nix, and Jack Muldoon for their tireless support on the report's editing, research, and data visualization.

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2026

Cover: German Chancellor Friedrich Merz and French President Emmanuel Macron attend a press conference on the day of a Summit on European Digital Sovereignty in Berlin, Germany, November 18, 2025. Source: REUTERS

Table of contents

Introduction

Over the past several years, the concept of digital sovereignty has become ever more central to European notions of competitiveness and economic resilience. Formerly a niche idea within the digital policy community, it has now gone mainstream with major European leaders, from European Commission President Ursula von der Leyen to former head of the European Central Bank Mario Draghi, calling for the European Union to achieve digital sovereignty.[1] It has also become integral to European debates about technological sovereignty and strategic autonomy, and even to trade policy. And as digital sovereignty has become more prominent in European discussions, it has shifted from being a vague aspiration to a concept that EU policymakers increasingly seek to put into operation—raising the possibility of future EU restrictions on procurement from companies outside Europe, as well as other regulatory measures.

Yet, despite its growing centrality in European digital debates, digital sovereignty still does not have a clear definition.[2] At times, it seems to have been encompassed by the broader term of tech sovereignty, which reflects the EU's desire to boost its industrial capabilities—not only in the digital space, but also in renewables and other green and future technologies. European policymakers also regularly refer to data sovereignty and cloud sovereignty, which can be seen as focused on particular aspects of digital sovereignty.

What all these definitions share, however, is the notion that Europe and its economy should be less dependent on others and more capable of protecting its own interests, including its interests in the digital sphere. That leads to the key unresolved questions at the heart of digital sovereignty. Does sovereignty require an economic approach that is exclusively European or, at minimum, favors European companies? Is ownership or effective control over key companies important, or is a risk-based system more appropriate? Is it desirable to limit sovereign requirements to certain sectors of the economy? Can Europe achieve a measure of sovereignty as part of a common enterprise among international partners? And if the partnership model is acceptable, who are the partners?

The transatlantic relationship is, in turn, entangled with Europe's internal debate about digital sovereignty. Until recently, this has been an evenly divided contest, with some European experts calling for Europe to strategically decouple from the dominance of US companies, while others—including most member-state governments—have noted the lack of local alternatives and hesitated to discriminate against US and other non-EU companies.

But the Donald Trump administration's initial open hostility to the EU and continuing general unpredictability have caused even the most transatlantic of EU leaders to question the reliability of the United States. The July 2025 US-EU trade deal provided some temporary clarity and predictability in transatlantic commercial relations, although digital issues were addressed in only limited ways. Trump's Truth Social post a few weeks later, threatening additional tariffs on countries with "Digital Taxes, Digital Services Legislation, and Digital Markets regulations [that] are all designed to harm, or discriminate against American Technology," was immediately criticized by the European Commission, France, Germany, and others as a violation of Europe's sovereignty.[3] Nevertheless, during a November 2025 visit to Brussels, Commerce Secretary Howard Lutnick directly linked the removal of EU digital regulation with a potential US-EU agreement on steel and aluminum tariffs.[4]

Given Trump's close connections with leading tech executives, the US administration's combative posture toward European tech regulation is likely to continue being a point of transatlantic friction. Whether a continued focus by the Trump administration on Europe's digital rules will create an even stronger push in Europe for an exclusive form of digital sovereignty is not yet evident. What is clear is that without some guidelines, such as those offered in the conclusions to this report, the European Union and United States might find that their differences regarding digital sovereignty and digital rules make creating and maintaining an open transatlantic digital marketplace much more challenging.

1 See, for example: "Von der Leyen Puts Digital Sovereignty at the Heart of EU's 2025 Agenda," Council of European Informatics Societies, September 16, 2025, https://cepis.org/von-der-leyen-puts-digital-sovereignty-at-the-heart-of-eus-2025-agenda/.

2 See the earlier work of the authors: Frances G. Burwell and Kenneth Propp, "The European Union and the Search for Digital Sovereignty: Building 'Fortress Europe' or Preparing for a New World?" Atlantic Council, June 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf; Frances Burwell and Kenneth Propp, "Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy," Atlantic Council, November 2, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/.

3 Donald J. Trump, Truth Social post, August 25, 2025, https://truthsocial.com/@realDonaldTrump/posts/115092243259973570; Elena Giordano, "EU Resists Trump: Tech Regulation Is Our 'Sovereign Right," *Politico*, August 26, 2025, https://www.politico.eu/article/eu-resists-trump-tech-regulation-is-our-sovereign-right/.

4 "Lutnick Talks EU Tech Rules, Nvidia H200 Chips, SCOTUS Tariff," Bloomberg, November 24, 2025, https://www.bloomberg.com/news/videos/2025-11-24/lutnick-talks-eu-tech-rules-nvidia-h200-chips-tariffs-video.

Defining the terms of the debate

One reason why digital sovereignty has become an increasingly inflammatory label across the Atlantic is that the lack of a clear definition allows everyone to define it in ways that support their own arguments. Its rise has also coincided with the European embrace of strategic autonomy in foreign and security policy—a notion that has predictably ruffled some US feathers, especially in the defense community. Further confusion has developed as similar terms (i.e., tech sovereignty, cloud sovereignty) have emerged in related areas. To introduce some clarity into this discussion, it can be useful to categorize these different notions.

Strategic autonomy: First arising in the context of foreign and security policy, strategic autonomy refers primarily to Europe developing defense and foreign policy capabilities that would allow the EU to play a more independent geopolitical role. Aside from a few defense funding efforts, the idea has not yet inspired major legislative initiatives. To indicate that partnership and autonomy were not contradictory, the EU later adopted the related idea of open strategic autonomy in trade policy. More recently, the EU has begun to embrace the concept of regulatory autonomy—the idea that "the Union's values, interests, and regulatory autonomy underpin EU action, including in the digital sphere."[5] In these notions, autonomy is a more ambiguous and flexible concept than sovereignty, which implies a legal order backed by legislative initiatives.

Technological sovereignty: While the first European Commission headed by von der Leyen focused largely on legislation related to the online world, the importance of technologies—and Europe's reliance on Chinese and US technologies—had come to the fore by the end of that mandate. This was not only about the digital world, but crucially about the European Green Deal. While the commission argued that carbon reduction would be key to the future EU economy, it became woefully clear that Europe remained dependent on others for many essential technologies: solar panels, wind turbines, semiconductors, electric vehicle batteries, etc.

Thus, in the second von der Leyen commission, the position of executive vice president for tech sovereignty, security, and democracy was created to oversee the development of EU capabilities to support the digital agenda. Others in the commission, including Executive Vice Presidents Teresa Ribera and Stéphane Séjourné, were tasked with strengthening EU technological capabilities across the Green Deal and industrial strategy generally. In June 2025, a key European Parliament committee defined tech sovereignty as "the ability to build capacity, resilience and security by reducing strategic dependencies, preventing reliance on foreign actors and single service providers, and safeguarding critical technologies and infrastructure."[6] Unlike strategic autonomy, however, tech sovereignty underlies significant legislative initiatives, from the Net Zero Industry Act and the Critical Raw Materials Act to the Public Procurement Directives. It also entails a strong focus on industrial policy, including state aid, competition policy, and other means of boosting key tech-related industries.

Figure 1: What constitutes European sovereignty in online spaces?

Digital sovereignty: While often used interchangeably with tech sovereignty, digital sovereignty focuses primarily on the

5 "European Council Meeting (23 October 2025) Conclusions," European Council, October 23, 2025, https://www.consilium.europa.eu/media/d2nhnqso/20251023-european-council-conclusions-en.pdf.

6 Sarah Knafo, "Report on European Technological Sovereignty and Digital Infrastructure," European Parliament, Committee on Industry, Research and Energy, June 11, 2025, https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html.

online world. Legislation such as the General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), and Artificial Intelligence Act (AIA) have sought to establish a comprehensive system of governance for the online world, especially by regulating corporate behavior vis-à-vis individual or business users. With the exception of semiconductors and the EU Chips Act, much less attention has been paid to the technologies that enable the online world. However, recent proposals for a Eurostack—a European capacity to provide all elements of digital infrastructure, from cables to cloud—are indications of growing European concern about both governance and technologies.[7]

Data sovereignty: This subset of digital sovereignty—one of the earliest variants—initially focused primarily on protection of personal data under the GDPR. However, with the Data Act and other initiatives, increased attention is now paid to the reuse of industrial data that are either sensitive or commercially valuable, and to safeguarding the capacity of EU businesses and governments to exploit data generated in Europe.

Cloud sovereignty: The proliferation of data requires enhanced storage capabilities and increased focus on cloud storage and the security of data stored in the cloud. An increasingly sharp debate has centered on whether Europeans' data should be stored exclusively within the EU, or whether they can be stored outside the EU by non-EU providers considered trustworthy and secure. This discussion has accelerated with the growth of artificial intelligence (AI) and its enormous requirements for cloud services and data centers. Cloud sovereignty also poses questions about how Europeans' data can be accessed by foreign law enforcement and intelligence agencies.

Figure 2: Europe's sovereignty equation

The EU'S Cloud Security Framework, published in October 2025, lays out eight "sovereignty objectives" for procurement authorities to score as they decide what cloud services and products to buy. Source: Cloud Security Framework, European Commission.

Sovereignty over speech: Users of online services today confront a wide array of illegal or undesirable content, from child sexual abuse material to advertisements for illegal products to political disinformation. EU efforts to regulate platforms' responsibility for illegal content and systemic risks have recently sparked criticism from the Trump administration, which regards aspects of these efforts as violations of free speech.[8] Who has the right to determine allowable speech available online in a jurisdiction other than where it was produced?

Cybersecurity: Given the ever-growing number of cyberattacks, both in Europe and globally, the protection of the online world has become a growing element in digital sovereignty. In the past, cybersecurity had not been central to the debate about digital sovereignty, but since the Russian full-scale invasion of Ukraine in 2022 there has been a rapidly growing understanding that resilience against such attacks is an essential part of sovereignty. Europe in particular has faced numerous attacks from Russia and related online actors. The EU effort to establish standards for cybersecurity has already led to US-EU tensions, but there will likely be even more attention paid to cyber-proofing as the EU operationalizes its concept of sovereignty.

As part of the growing effort to operationalize digital sovereignty, both EU institutions and member states have initiated efforts to elaborate the meaning of this elusive concept. The European Council, in formal conclusions to its October 23 meeting, declared, "It is crucial to advance Europe's digital transformation, reinforce its sovereignty, and strengthen its own open digital ecosystem," adding that "this requires reinforced international partnerships and close collaboration with trusted partner countries."[9]

On November 18, 2025, the French and German governments convened a Summit on European Digital Sovereignty. The summit identified several areas for building digital sovereignty, including AI, data, and public infrastructure, and launched a joint task force on European digital sovereignty to report in

7 Cristina Caffarra, et al., "Deploying the Eurostack: What's Needed Now," Eurostack Initiative, May 19, 2025, https://eurostack.eu/wp-content/uploads/2025/08/eurostack-white-paper-final-19-05-25-3.pdf.

8 Kenneth Propp, "Talking Past Each Other: Why the US-EU Dispute over 'Free Speech' Is Set to Escalate," Atlantic Council, August 15, 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/us-eu-dispute-over-free-speech-is-set-to-escalate/.

9 "European Council Meeting (23 October 2025) Conclusions."

European officials pose for a family photo at the Summit on European Digital Sovereignty in Berlin, Germany, November 18, 2025. Source: REUTERS/Nadja Wohlleben.

2026.[10] Its final declaration underscored the EU member states' "shared ambition to strengthen Europe's digital sovereignty in an open manner as a cornerstone of our economic resilience, social prosperity, competitiveness and security."[11]

The European Commission, for its part, issued a Cloud Sovereignty Framework in September 2025 that identifies eight types of sovereignty-related objectives to be considered in the government procurement context. In a stab at precision, contracting authorities should assign each objective a sovereignty effective assurance level (SEAL). The results of that assessment should provide a mathematically derived sovereignty score.[12] But as EU discussions on this topic progress, there are still key differences among the member states about the choice between strict autonomy or international partnerships, and whether the model should be based on exclusive EU control or on risk management.

10 "Summit on European Digital Sovereignty Delivers Landmark Commitments for a More Competitive and Sovereign Europe," Élysée, November 18, 2025, https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe.

11 "Declaration for European Digital Sovereignty," Council of the European Union, December 5, 2025, https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf.

12 "Cloud Sovereignty Framework," European Commission, October 2025, https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf.

Europe's missing Silicon Valley

While many non-European observers would say that the EU's regulatory power already gives it significant influence domestically and externally, the EU's sovereignty in the European digital arena is vulnerable at best. Despite its role as a regulatory superpower, Europe finds itself reliant on non-EU companies for many essential elements of the digital world. A European Parliament report estimates that "the EU relies on non-EU countries for over 80% of digital products, services, infrastructure, and intellectual property."[13] This perception of dependency is at the heart of the EU push for digital sovereignty.

The EU has failed to develop a tech sector with either the vibrancy of Silicon Valley or the growing capabilities of China's industry. In particular, Europe has not seen the emergence of world-leading new companies based on digital technologies. Indeed, while the US industry has created six companies with a market capitalization of €1 trillion or more, the EU has created none.[14] In 2021, three US cloud companies supplied 65 percent of the EU cloud market, while EU-headquartered companies had less than 16 percent.[15] As a consequence, European consumers and businesses must rely on non-EU companies—mostly US and some Chinese enterprises—for basic digital services. Initially, this largely applied to software, social media, search engines, and a wide array of shopping services. More recently, the importance of cloud, encryption, and AI, along with the prospective emergence of super-fast quantum computing, has made Europeans realize that this dependence on others has significant and potentially long-lasting effects on their own industries and economies, including those far beyond the tech sector.

Of course, a few European companies are exceptions to these trends. Nokia and Ericsson were already leaders in the cables and fiber optics that are key to connectivity. They became even stronger in the market as concerns rose about the security of Chinese components. The Dutch company ASML has been a leader in the machines required to make the semiconductors that guide and manage so much of the digital world. SAP is the world's largest vendor of enterprise resource planning software. But these European companies are not in the same league as their US equivalents in terms of market capitalization. For example, ASML has a market capitalization of $376 billion, while Nvidia is at $4.3 trillion and Microsoft is at $3.8 trillion.[16]

One consequence of Europe's struggle in the digital marketplace has been the emergence of an EU-wide debate on competitiveness, as represented most prominently by the reports by former Italian Prime Minister Enrico Letta and former head of the European Central Bank Mario Draghi.[17] Draghi specifically underlined the importance of Europe's failure to develop an innovative tech sector by noting the increasing productivity gap between the EU and the United States, with European labor productivity falling to 80 percent of US productivity. He

US Ambassador to the EU Andrew Puzder highlights the disparity between major companies founded in the United States and the EU at the 2025 Transatlantic Forum on GeoEconomics, in Brussels, on September 30, 2025. Source: Nicolas Lobet, PRYZM photography.

13 Knafo, "Report on European Technological Sovereignty and Digital Infrastructure."

14 Mario Draghi, "The Future of European Competitiveness," European Commission, September 9, 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

15 Ibid.

16 "Largest Tech Companies by Market Cap," CompaniesMarketCap, last visited September 27, 2025, https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/.

17 Enrico Letta, "Much More than a Market," European Council, April 2024, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf.

European Commission President Ursula von der Leyen holds former head of the European Central Bank Mario Draghi's report on EU competitiveness at a September 2024 press conference in Brussels. Draghi's report concluded that Europe failed to capitalize on the emergence of the internet to increase productivity. Source: REUTERS/Yves Herman.

concluded that this was mainly due to "Europe's failure to capitalise on the first digital revolution led by the internet—both in terms of generating new tech companies and diffusing digital tech into the economy."[18]

The competitiveness debate has also sought to identify the causes of Europe's lack of digital champions. Europe has a vibrant startup community, as demonstrated by the growing role of venture capital.[19] But many of these innovative enterprises end up moving to the United States or elsewhere, while others fail to commercialize entirely. The most popular rationale for this failure to scale—cited by US and European analysts, including Draghi—is overregulation.[20] Other suggested reasons include a chronic lack of indigenous capital, overly strict bankruptcy laws, and a culture that fears failure.[21] Whatever the reason, Europe's inability to provide the resources and capabilities for its innovative companies to become continental champions, let alone world leaders, means it must rely on companies from elsewhere.

This was already the case in 2018, when the GDPR—the first major piece of EU digital legislation—came into force. During the next five years of von der Leyen's first term as commission president, the EU passed several other pieces of digital

18 Draghi, "The Future of European Competitiveness."

19 Ivan Levingston, "European Start-up Valuations Boom on Investor Frenzy," *Financial Times*, September 5, 2025, https://www.ft.com/content/5cd37cea-87e7-4648-b85b-f77091dd4558.

20 Draghi, "The Future of European Competitiveness."

21 Ramsha Jahangir, "What's Behind Europe's Push to 'Simplify' Tech Regulation?" Tech Policy Press, April 24, 2025, https://www.techpolicy.press/whats-behind-europes-push-to-simplify-tech-regulation/.

legislation, most notably the DSA, DMA, and AIA. These measures made progress in harmonizing diverse member-state laws, both existing and anticipated. But while EU leaders saw this body of legislation as protecting their citizens from the excesses of data collection and illegal social media content, many outside the EU, especially in the US tech community, viewed these laws as overly burdensome at best and discriminatory at worst. Some EU policymakers, such as Member of the European Parliament (MEP) Andreas Schwab, early on were open about their desire to counter the dominance of US firms.[22] Others, however, saw Europe as offering a positive alternative to the lightly regulated environment tech companies faced elsewhere. EU rules inevitably had the most impact on US companies, which provided the overwhelming majority of digital services in the EU market. Chinese companies also came to feel the impact of EU regulations as their market share grew over time, especially in shopping and social media.

Throughout this period of intense legislative activity, there were clear voices calling for greater digital sovereignty in Europe. The body of legislation passed in the first von der Leyen commission can certainly be viewed as an effort to place limits on the US companies that dominate Europe's digital space—and as a way for Europe to regain some control, or sovereignty, over that market. But as competitiveness emerged as a top EU priority in 2023, the discussion about digital sovereignty became part of a much broader discussion about innovation and economic security.

Geopolitics and the rise of tech sovereignty

The earliest indication of a geopolitical element to EU digital sovereignty came during the first Trump administration, when the United States protested the use of Huawei components in European digital networks. Reluctantly at first, Europeans came to understand the risk of a Chinese capability to disrupt those networks and developed the EU Toolbox for 5G Security, a list of best practices released in January 2020. The toolbox identified states and state-backed actors as the most serious threats. It also set out criteria for identifying trusted versus untrusted vendors, including closeness to a foreign government, lack of democratic accountability in that government, lack of a data protection agreement with the EU, and ability of the third country to exercise pressure on the EU.[23]

The toolbox was the first real effort to identify foreign companies and governments that might threaten Europe's digital sovereignty and those that might not. There was clearly a focus on China and Chinese companies, as demonstrated by the criteria for vendors. But it should be noted that the toolbox is primarily voluntary guidance developed by the member states for themselves, with progress tracked by regular EU Commission reporting.

In 2019, the EU identified China as both an economic competitor and a "systemic rival," but initially with little consequence, especially in terms of economic relations.[24] Over the next few years, the EU would increasingly focus on China and the dangers posed by its investments in the European economy, especially in critical European infrastructure. By March 2023, when von der Leyen called for de-risking Europe from China,[25] commission officials had identified a number of EU dependencies on China—including in critical raw materials, solar panels, and batteries—that had the power to disrupt European industry.[26] In June 2023, the commission reported that it considered Huawei and ZTE "materially higher risks" than other fifth-generation (5G) suppliers."[27]

The EU also initiated a few measures to address those vulnerabilities: heightened screening of inward foreign investment, primarily at the member-state level; enactment

22 Javier Espinosa, "EU Should Focus on Top 5 Tech Companies, Says Leading MEP," *Financial Times*, May 31, 2021, https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b.

23 "Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigation Measures," European Commission, January 23, 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

24 "EU–China—A Strategic Outlook," European Commission and European External Action Service, March 12, 2019, https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf.

25 "Speech by President von der Leyen on EU-China Relations to the Mercator Institute for China Studies and the European Policy Centre," European Commission, March 29, 2023, https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2063.

26 "Strategic Dependencies and Capacities," European Commission, May 5, 2021, https://commission.europa.eu/system/files/2021-05/swd-strategic-dependencies-capacities_en.pdf.

27 "Commission Announces Next Steps on Cybersecurity of 5G Networks in Complement to Latest Progress Report by Member States," European Commission, press release, June 14, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309.

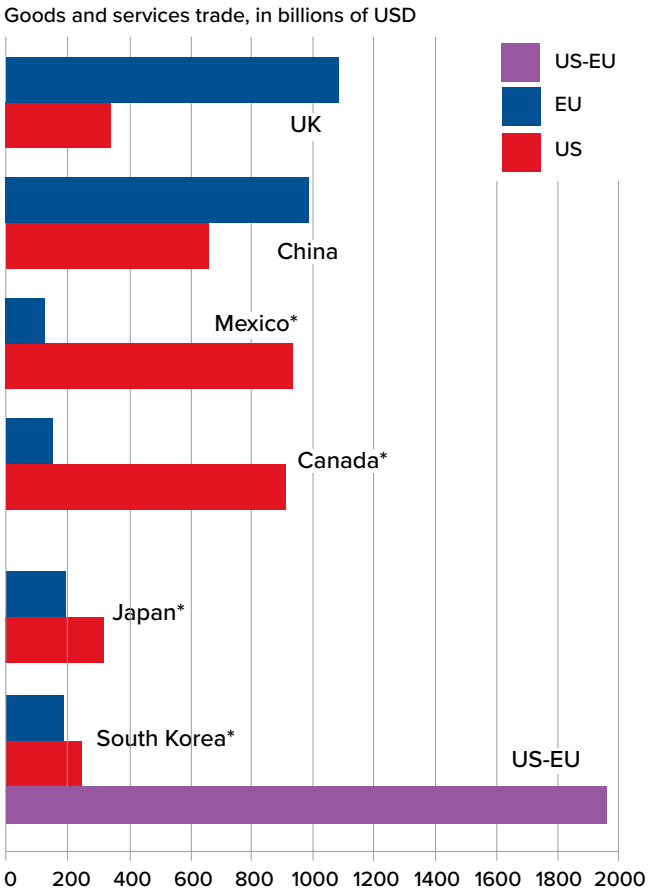
of the European Chips Act, providing funding for advanced semiconductor manufacturing in Europe; adoption of the Critical Raw Materials Act, which established goals for EU production of key materials; and passage of the Net Zero Industry Act, which sought to build EU manufacturing capacity in clean technologies such as solar, batteries, and hydrogen. While these measures were not aimed only at China, concerns about that country's ambitious global plans were a main motivation. Moreover, they had the effect of broadening the initially limited discussion of digital sovereignty beyond the realm of digital governance to include both digital and green technologies, resulting in a broader focus on technological sovereignty.

This European debate regarding the geopolitical dimensions of sovereignty—both digital and tech—intensified significantly following the Russian invasion of Ukraine in February 2022. Along with a focus on territorial security, as seen in the increased defense spending of most EU member states, the EU realized that it needed to address other vulnerabilities. Most urgently, the invasion led to a swift and drastic shift in Europe's energy supply, as Russia went from providing 45 percent of Europe's oil and gas in 2021 to 19 percent in 2024.[28] But the digital arena was also vulnerable: Russian cyberattacks and apparent sabotage against undersea cables demonstrated the dangers facing Europe's digital infrastructure, while Russian-origin disinformation flooded European social media.

Perhaps the most important consequence of the Russian invasion, however, was the realization that Europe was vulnerable and that preserving its sovereignty—digital and otherwise—would require concrete actions. Many of the green technology initiatives mentioned above were still in the legislative process when the invasion began but moved to enactment by mid-2023 as the commission's term began to close and as Europeans became even more conscious of those vulnerabilities. Competitiveness, resilience, and sovereignty became linked together in the concept of economic security as the EU sought to reduce its external dependencies, especially on Russia and China.

By the end of 2024, the tech sovereignty impulse in Europe had become a key policy priority, as demonstrated by the appointment of Henna Virkkunen to the new position of European Commission executive vice president for tech sovereignty, security, and democracy. But before the second von der Leyen commission could get its program under way—or make progress in implementing the Draghi report—Trump's reelection as US president pushed the impulse toward European digital sovereignty into hyperdrive.

Figure 5: Major bilateral trade relationships



Source: US Trade Representative; EU Commission
*For respective EU data, trade valuations total most recent available data, including 2024 trade in goods and 2023 trade in services.
All US data is from 2024.

28 "Roadmap Towards Ending Russian Energy Imports," European Commission, May 12, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0440R(01).

Trump actions spur renewed calls for greater independence

European suspicions about US intentions and capabilities in the digital world have existed since 2013, when Edward Snowden revealed the extent of US National Security Agency interception of Europeans' communications. Nevertheless, the United States and EU enjoyed relatively open trade in digital services. The advent of the second Trump administration, however, has energized the transatlantic debate over digital sovereignty. While Trump's focus during the 2024 campaign was on the EU's trade in goods surplus with the United States, once back in office he frequently criticized the EU's digital regulations as a whole, despite the US surplus in services trade driven by the success of US tech companies.

Such an aggressive approach brought the issue of digital sovereignty to the fore, as it seemed to disregard the EU's right to regulate its own market. As the United States and EU pursued a trade agreement, there were conflicting reports as to whether the DSA and DMA (as well as other EU regulations) were on the negotiating table.[29] In the end, the joint statement published on August 21, 2025, did not mention either regulation or the DSTs adopted by several EU member states.

But the joint statement was hardly the last word. On August 25, Trump posted on Truth Social: "As the President of the United States, I will stand up to Countries that attack our incredible American Tech Companies. Digital Taxes, Digital Services Legislation, and Digital Markets Regulations are all designed to harm, or discriminate against, American Technology."[30] Meanwhile von der Leyen, in her September 2025 State of the Union speech, defended the trade deal but also stated: "Whether on environmental or digital regulation, we set our own standards. We set our own regulations. Europe will always decide for itself."[31]

The Trump administration has continued criticizing EU digital regulation. For example, on December 16, US Trade Representative Jamieson Greer posted on X (formerly Twitter) that the EU had "persisted in a continuing course of discriminatory and harassing lawsuits, taxes, fines, and directives against U.S. service providers," and suggested that the United States would retaliate.[32] It would be relatively easy for the administration to renew the Section 301 investigations of DSTs. The US government might also look for a mechanism to counter the impact of the DSA and DMA, especially if US companies are fined significantly under those laws. On April 23, 2025, the European Commission fined Apple and Meta €500 million and €200 million, respectively, for noncompliance with the DMA.[33] In September, Google was fined €2.95 billion for "distorting competition in the advertising technology industry," although this case was pursued under the European Commission's long-time competition authorities rather than under the DMA.[34]

The commission is also investigating X as well as Meta's Facebook and Instagram for alleged violations of the DSA, along with separate probes of the Chinese firms AliExpress, Temu, and Tiktok, and several European-based online pornography platforms. On December 5, 2025, the Commission fined X €120 million under the DSA for issues related to its blue checkmarks and advertising repository.[35] Beyond these specific cases, the growing criticism of Europe from the US executive branch and parts of Congress, which claim it is censoring "free speech," is an indication that an influential segment of the Republican Party in the United States will continue to push for action against European efforts to moderate digital content. The EU has been a key target, as has the United Kingdom with its Online Safety Act.

At the same time, the European Commission has embarked on a process of simplifying some regulations as part of an effort to make the EU economy more competitive. A digital omnibus—a legislative package designed to amend several regulations across a sector simultaneously—was presented

29 Alice Hancock, Paola Tamma, and James Politi, "EU Push to Protect Digital Rules Holds Up Trade Statement with US," *Financial Times*, August 17, 2025. https://www.ft.com/content/3f67b6ca-7259-4612-8e51-12b497128552.

30 Truth Social, August 25, 2025.

31 "2025 State of the Union Address by President von der Leyen," European Commission, September 9, 2025, https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053.

32 United States Trade Representative (@USTradeRep), X post, December 16, 2025, https://x.com/USTradeRep/status/2000990028835508258.

33 "Commission Finds Apple and Meta in Breach of the Digital Markets Act," European Commission, press release, April 23, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-finds-apple-and-meta-breach-digital-markets-act.

34 "Commission Fines Google €2.95 Billion over Abusive Practices in Online Advertising Technology," European Commission, press release, September 4, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992.

35 "Commission fines X €120 million under the Digital Services Act," European Commission, press release, December 5, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act.

US Trade Representative Jamieson Greer and US Commerce Secretary Howard Lutnick speak after a meeting with the EU Trade Ministers Council in Brussels on November 24, 2025. Lutnick suggested that the EU "reconsider" some digital regulations if the bloc wanted the United States to reduce tariffs on EU steel and aluminum. REUTERS/Piroschka van de Wouw.

on November 19, 2025.[36] As with other commission proposals for simplifying regulations, the digital omnibus focuses on reducing requirements for small and medium-sized enterprises (SMEs), along with streamlining reporting in cases of cybersecurity incidents. It also proposes delaying implementation of AIA requirements for high-risk systems until relevant guidance has been issued and calls for "targeted amendments" to the GDPR to boost innovation, including that related to AI training.[37] While simplification is likely to reduce the regulatory burden on tech companies in Europe—including large US companies—it has not yet addressed issues related to digital sovereignty.

Apart from potential revisions to existing legislation, the commission plans to move forward on two tracks. First, the second von der Leyen commission anticipates deploying more financial resources to support research on emerging technologies such as AI and quantum. Early in 2025, von der Leyen announced InvestAI, an initiative to raise €200 billion in investment capital.[38] The EU also plans, through the 2025 EU Startup and ScaleUp Strategy, to support startups in their search for the funding that will allow them to grow.[39] While these funds should be viewed with some caution—it is unclear whether sufficient private funds will join this public-private effort—they demonstrate the EU's commitment to building its own capabilities.

36 Mark MacCarthy and Kenneth Propp, "The European Union Changes Course on Digital Legislation," Lawfare, December 15, 2025, https://www.lawfaremedia.org/article/the-european-union-changes-course-on-digital-legislation.

37 "Simpler EU Digital Rules and New Digital Wallets to Save Billions for Businesses and Boost Innovation," European Commission, press release, November 19, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718.

38 "EU Launches InvestAI Initiative to Mobilise €200 Billion of Investment in Artificial Intelligence," European Commission, press release, February 10, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467.

39 "Commission Launches Ambitious Strategy to Make Europe a Startup and Scaleup Powerhouse," European Commission, press release, May 27, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1350.

Second, the commission has made clear that it will continue to pursue new rules governing activities and companies in the digital arena. The Financial Data Access (FiDA) regulation, now in the final stage of negotiations, is intended to allow greater sharing of financial data among financial institutions in order to develop new digital financial products for consumers. European legacy banks have launched an effort to exclude those companies designated as gatekeepers under the Digital Markets Act from participation in FiDA; this effort will primarily affect US tech companies.[40]

The EU Cloud and AI Development Act (CADA) will attempt to address the EU's shortcomings in cloud and AI capacity by encouraging the permitting of new data centers and other infrastructure, and by providing greater computational capacity and resources to startups, especially those focused on AI. But it is also expected to establish EU-wide eligibility requirements for cloud service providers, along with harmonized procurement processes, in ways that could restrict participation by non-EU companies. It is not clear yet whether CADA will address concerns through risk-based assurance models or ownership restrictions. It has reportedly been delayed until the first quarter of 2026 as the commission considers the concept of European effective control as a way of supporting EU digital sovereignty.[41]

The Digital Fairness Act, expected to be introduced in mid-2026, will be the EU's flagship legislation for business-to-consumer relations and will address protection of minors online, transparent online pricing, the abuses of manipulative and addictive design, and marketing by influencers—all of which are likely to be of significant interest to US platforms. Other initiatives expected to be launched in the next eighteen months include the ICT Supply Chain Toolbox, the Quantum Europe Strategy, and the Digital Networks Act. Finally, the European Data Union Strategy, released on November 19 along with the digital omnibus, establishes the ambition of "safeguarding the EU's data sovereignty through a strategic international data policy."[42] It aims to do this by "making fair conditions for data access and cross-border transfer . . . protecting sensitive EU non-personal data . . . and deepening cooperation with trusted partners."[43] While a strategy is not a legislative document, we can expect that it will help guide EU policy on international data flows.

The European Parliament is also active in the digital sovereignty debate. MEP Axel Voss, one of the parliament's leaders on these issues, wrote in an October 2025 post on LinkedIn: "We need immediate decisions to regain a digitally competitive and sovereign EU. Eurostack, deregulation, venture capital, chips, energy, access to quality data and a flourishing environment for Start Ups and creators are crucial for our sovereignty."[44] He proposes a number of measures, from digital special economic zones to using only EU programs within EU institutions to integrating "buy and deploy European tech" in public procurement.[45]

These initiatives will undoubtedly continue to have an impact on the transatlantic relationship, as they will affect the major actors in the market, most of them American. Even with the best of intentions—and no ambition to exclude those companies—EU adoption and implementation of such rules will likely raise questions about the openness of its future market and the participation of non-EU firms.

The next section explores how the United States and EU have wrestled with the competing pressures of sovereignty and open markets, as presented by a set of key issues relating to government access to data.

40 Barbara Moens and Paola Tamma, "EU to Block Big Tech from New Financial Sharing Data System," *Financial Times*, September 21, 2025, https://www.ft.com/content/6596876f-c831-482c-878c-78c1499ef543.

41 Luca Bertuzzi, "'Effective control' concept for cloud sovereignty eyed by EU Commission," MLex, September 4, 2025, https://www.mlex.com/mlex/articles/2384011/-effective-control-concept-for-cloud-sovereignty-eyed-by-eu-commission?trk=public_post_comment-text.

42 "European Data Union Strategy," European Commission, November 19, 2025, 18–20, https://digital-strategy.ec.europa.eu/en/policies/data-union.

43 Ibid.

44 Axel Voss, "Regaining Europe's Digital Sovereignty: Ten Immediate Actions for 2025," EPP Group at the European Parliament, October 7, 2025, https://www.axel-voss-europa.de/wp-content/uploads/2025/10/AVoss-10-Steps-Digital-Sovereignty.pdf.

45 Ibid.

Figure 3: EU digital and tech initiatives

Artificial Intelligence Act	Aims to regulate the development and use of AI, especially "high-risk" AI.	Phased application since February 2025.
Common Chargers Rule in Radio Equipment Directive	Establishes common charging ports for manufacturers of portable electronic devices.	Applicable since December 2024.
Communication on a European Strategy for Data	Outlines the European Commission's plans to create a single market for data that will enable EU innovation and competitiveness.	Published February 2020.
Communication on a New Industrial Strategy for Europe	Outlines the EU's plan to use the green and digital transitions to make EU industry more competitive globally and to enhance the EU's strategic autonomy.	Published March 2020.
Cyber Resilience Act	Establishes cybersecurity rules on connected products and services for manufacturers and vendors.	In force; phased application underway.
Data Act	Aimed at stimulating EU innovation and competitiveness through the development of a market for non-personal, industrial data	Applicable from September 2025.
Data Governance Act	Facilitates the sharing of public sector, non-personal data to enhance innovation in the EU.	Applicable since September 2023.
Digital Fairness Act	Modernizes digital consumer law by tackling dark patterns, addictive design, misleading influencer marketing and unfair personalization.	Under preparation; consultations completed 2025, draft regulation and proposal expected 2026.
Digital Markets Act (DMA)	Establishes specialized competition rules for large digital platforms identified as "gatekeepers."	Applicable since May 2023.
Digital Networks Act	Reforms telecoms to boost investment in very high capacity networks, modernize rules, and strengthen security and resilience of EU digital infrastructure.	Pre-proposal; stakeholder consultations completed, Commission proposal expected early 2026.
Digital Services Act (DSA)	Retains intermediate liability protections for online platforms but also established common rules for platforms' content moderation and reporting requirements.	Applicable since February 2024.
Directive on Copyright in the Digital Single Market	Requires online platforms to provide remuneration for creators and publishers when their content is used online.	In force; member state transposition completed.
Directive on Security of Network and Information Systems (NIS2)	Updates cybersecurity and reporting requirements for companies providing critical infrastructure and services, including online marketplaces, search engines, and cloud services.	In force; infringement proceedings against non-compliant member states ongoing.
European Chips Act	Develops the EU's semiconductor capacity with government subsidies and public and private investments.	Adopted; funding and implementation underway.
EU Cloud and AI Development Act (CADA)	Aims to triple EU data-center capacity and securing energy-efficient cloud and HPC infrastructure.	Pre-legislative; consultations completed 2025, Commission proposal planned for early 2026.
EU Cybersecurity Act	Establishes a cybersecurity certification framework and expands remit of the EU's cyber agency, ENISA.	In force since June 2019.
European Data Union Strategy	Updates EU data strategy by rationalizing the EU's data-rule landscape, boosting access to high-quality data, and positioning the EU in global data-flow governance.	Adopted November 2025; implementation via follow-up initiatives and targeted legislation 2026–27.

European Democracy Action Plan	Outlines anticipated proposal for legislation governing political ads and other rules intended to safeguard democratic processes, including elections.	Published; implemented through political advertising rules.
2025 EU Startup and ScaleUp Strategy	Removes barriers for young firms by improving access to finance, markets, and regulation.	Non-binding framework; implemented via EIC, ESCALAR, Competitiveness Compass, and AI Continent initiatives.
Financial Data Access (FiDA) regulation	Creates EU-wide rules for customer-permissioned sharing of financial-sector data beyond payment accounts, enabling standardized data-sharing schemes.	Council position adopted 2024; trilogue ongoing, final adoption expected in 2026.
General Data Protection Regulation	Governs the collection, processing, and transfer of personal data located in EU territories.	Applicable since May 2018 across EU.
ICT Supply Chain Toolbox	Identifies ICT supply chain risks and recommends coordinated strategic and technical measures for entities covered by the NIS2 Directive.	Non-binding toolbox; drafted 2025, feeding into coordinated risk assessments and Cybersecurity Act review.
InvestAI	Mobilizes €200bn for AI Investment, including a European fund for "AI gigafactories" to build shared compute infrastructure.	Announced February 2025; funding structures and project pipelines developed during 2025–26.
Product Liability Directive Revision	Updates liability rules on product risks associated with digital and green transitions.	Adopted; member state transposition ongoing.
Public Procurement Reform	Revises public procurement directives to extend and simplify binding non-pricing criteria and use joint procurement to build strategic stockpiles of critical materials.	Consulation period open with proposal expected in late 2026.
Scaleup Europe Fund	Channels late-stage capital into European tech scale-ups via a Commission–EIB public–private fund.	Announced 2025; fund setup ongoing, first closings and investments expected from 2026.,

Snowden's revelations and the 'kill switch'

More than a decade has passed since the Snowden revelations, but the topic continues to shadow transatlantic digital relations. Many in Europe hailed Snowden as a hero for revealing Europe's vulnerability to US signals intelligence, and the European Parliament invited him to appear and speak at a plenary meeting. The Barack Obama administration, which charged Snowden under the Espionage Act, objected vehemently to the invitation and, in the end, Snowden addressed the parliament only by video link.[46] Now, however, US domestic sentiment regarding Snowden's actions has begun to shift, at least in Republican circles, as several of Trump's advisers have called for him to be pardoned.[47]

Snowden's disclosures started a chain of legal proceedings in Europe that generated substantial uncertainty among companies about the legality of their indispensable transfers of personal data to the United States. The Court of Justice of the European Union (CJEU) twice invalidated EU-US international transfer arrangements, judging them insufficient to protect Europeans' fundamental rights. In 2015, the court

46 Peter Finn and Sari Horwitz, "US Charges Snowden with Espionage," *Washington Post*, June 21, 2013, https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html; Dave Keating, "European Parliament to Hear Snowden testimony," *Politico*, January 9, 2014, https://www.politico.eu/article/european-parliament-to-hear-snowden-testimony/.

47 Michael Scherer, "Trump Advisers Renew Push for Pardon of Edward Snowden," *Washington Post*, December 4, 2024, https://www.washingtonpost.com/politics/2024/12/04/trump-pardon-edward-snowden-gaetz/.

struck down the EU-US Safe Harbor Framework, and a successor arrangement, the Privacy Shield, met the same fate in 2020.[48] Meta, the object of the litigation both times, took the issue seriously enough that it publicly conceded to US securities regulators that it might need to withdraw Facebook and Instagram from Europe if it could not legally transfer data to the United States.[49]

A third arrangement, the EU-US Data Privacy Framework (DPF), concluded in 2023, put significant additional safeguards in place for Europeans' personal data when they are transferred to the United States. It has stabilized the situation, at least for the time being. On September 3, 2025, the EU General Court rejected a challenge to the DPF brought by Philippe Latombe, a French parliamentarian.[50] The case tested the sufficiency of US legal reforms made to overcome the CJEU's 2020 judgment on the Privacy Shield. The court rejected claims that a redress mechanism created by the agreement lacked independence within the US legal system. It also validated the sufficiency of US safeguards relating to the collection of bulk data for intelligence purposes. Latombe has appealed the General Court verdict to the Court of Justice, however, so a definitive verdict on the fate of DPF has yet to be issued.[51]

The European privacy advocacy organization None of Your Business (NOYB)—headed by well-known Austrian privacy activist Max Schrems, who brought the 2015 and 2020 CJEU cases—reacted with disbelief to the Latombe ruling. Schrems drew attention to Trump administration actions against the independence of the US Privacy and Civil Liberties Oversight Board (PCLOB) and the Federal Trade Commission (FTC). He also said that he is mulling bringing a second challenge to the DPF in EU courts.[52]

US cloud service providers, including Amazon Web Services and Microsoft, have responded to European unease over data transfers to the United States by introducing service features that allow enterprise customers to store certain types of data exclusively on servers located on the continent.[53] Offering to localize data in this fashion can reassure European customers concerned about the long arm of US government's potential access to their data.

However, the Trump administration exacerbated European anxiety over data flows to and from the United States by briefly cutting off Ukraine from US intelligence sharing in early 2025.[54] The specter of a US government kill switch—in the form of an order to US cloud providers to stop commercial data transfers to Europe—has spurred further efforts by US cloud providers to reassure their European customers. Brad Smith, Microsoft's vice chair and president, went so far as to issue a public statement in April that, "In the unlikely event we are ever ordered by any government anywhere in the world to suspend or cease cloud operations in Europe, we are committing that Microsoft will promptly and vigorously contest such a measure using all legal avenues available, including by pursuing litigation in court."[55]

In response, some European companies have spied a business opportunity. For example, the German company Ecosia and its French counterpart Qwant announced their intention to build

48 Schrems v. Data Protection Commissioner, CASE C-362/14 (Court of Justice of the EU 2015), https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2522200; Data Protection Commissioner v. Facebook Ireland & Schrems, CASE C-311/18 (Court of Justice of the EU 2020), https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4010715.

49 "Meta Platforms, Inc. Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1933 for the Fiscal Year Ended on December 31, 2022," US Securities and Exchange Commission, 2022, https://www.sec.gov/Archives/edgar/data/1326801/000132680123000013/meta-20221231.htm.

50 "Data Protection: The General Court Dismisses an Action for Annulment of the New Framework for the Transfer of Personal Data between the European Union and the United States," Court of Justice of the European Union, press release, September 3, 2025, https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250106en.pdf.

51 Claudie Moreau and Théophane Hartmann, "Latombe to Appeal EU-US Data Transfer Court Challenge," Euractiv, October 29, 2025, https://www.euractiv.com/news/exclusive-latombe-to-appeal-eu-us-data-transfer-court-challenge/.

52 "EU-US Data Transfers: First Reaction on 'Latombe' Case," Noyb, September 3, 2025, https://noyb.eu/en/eu-us-data-transfers-first-reaction-latombe-case.

53 Matt Garman and Max Peterson, "AWS Digital Sovereignty Pledge: Announcing a New, Independent Sovereign Cloud in Europe," AWS Security Blog, October 24, 2023, https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-announcing-a-new-independent-sovereign-cloud-in-europe/; Julie Brill and Erin Chapple, "Microsoft Announces the Phased Rollout of the EU Data Boundary for the Microsoft Cloud Begins January 1, 2023," Microsoft EU Policy Blog, December 15, 2022, https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/.

54 Emily Benson, Max Bergmann, and Federico Steinberg, "The Transatlantic Tech Clash: Will Europe 'De-Risk' from the United States?" Center for Strategic and International Studies, May 2, 2025, https://www.csis.org/analysis/transatlantic-tech-clash-will-europe-de-risk-united-states.

55 Brad Smith, "Microsoft Announces New European Digital Commitments," Microsoft, April 30, 2025, https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments.

a European web index called European Search Perspective (ESP) to compete with Google's search engine.[56] Ecosia's chief executive officer (CEO) cited concern about the political winds blowing in the United States: "With the US election turning out as it has, I think there is an increased fear that the future US president will do things that we as Europeans don't like very much . . . We, as a European community, just need to make sure that nobody can blackmail us."[57] He also emphasized Europe's current dependence on Google's services: "If the US turned off access to search results tomorrow, we would have to go back to phone books."

The European dream of regaining data sovereignty by generating companies that can compete with the US cloud giants has a long history of failure. Our 2022 report chronicled the ambitious Franco-German effort to develop GAIA-X, a federated data and cloud ecosystem.[58] In the years since, the vision of an interoperable network of trusted European cloud providers has had limited success. Its major output is a series of standards, specifications, and labels for European cloud providers, rather than a transformation of the commercial landscape.[59]

Draghi's 2024 report on the single market effectively conceded defeat in this area of endeavor. "It is too late for the EU to . . . develop systematic challengers to the major US cloud providers," Draghi wrote.[60] Nonetheless, European anxiety over the possibility, however small, that dominant US platform services could withdraw from the continent, be blocked from serving it by the US government, or be a mechanism for channeling EU data to the US government, will continue to power a push for European sovereign alternatives.

A second continuing impetus is an awareness in Europe—thanks to Snowden—that the dominance of US digital services in Europe offers US intelligence agencies a strategic advantage. The Joe Biden administration even boasted of this during the 2023 congressional debate to reauthorize Section 702 of the Foreign Intelligence Surveillance Act (FISA), a principal authority for collecting intelligence information on non-Americans. The pervasiveness of US digital service providers worldwide, the administration noted, allows US intelligence agencies to "leverage this national advantage to collect foreign intelligence information . . . in order to protect America from its adversaries."[61]

US law enforcement access to data on European servers

US intelligence collection in Europe is not the only challenge to data sovereignty that the EU sees emanating from the United States. Another is the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), a 2018 US law. This statute confirmed that US law enforcement can unilaterally order cloud service providers with a presence in the United States to turn over personal data they host on servers in Europe and other foreign locations for criminal investigations and prosecutions. Although several EU countries, including Belgium, give their law enforcement authorities similar extraterritorial criminal evidentiary powers, this part of the CLOUD Act is seen in Europe as singularly intrusive. When EU legislators call for companies to be immune to foreign law, they are often referring to the CLOUD Act.

However, the CLOUD Act also contains a conciliatory dimension. Part II of the act authorizes the US Department of Justice to negotiate binding international agreements under which criminal investigators and prosecutors can obtain foreign-located electronic evidence directly from providers. Because CLOUD Act agreements are consensual, they do not violate a foreign state's judicial sovereignty by commanding that a legal measure be taken on its territory. Instead, they remove legal obstacles that companies otherwise face in voluntarily assisting foreign law enforcement. This new type of international agreement can substantially reduce reliance on mutual legal assistance treaties (MLATs), which can be too slow and cumbersome for obtaining e-evidence in fast-moving investigations.

56 Alex Matthews, "Can Europe Build Itself a Rival to Google?" Deutsche Welle, December 9, 2024, https://www.dw.com/en/european-search-engines-ecosia-and-qwant-to-challenge-google/a-70898027.

57 Ibid.

58 Burwell and Propp, "Digital Sovereignty in Practice."

59 Mathieu Pollet, "Anatomy of a Franco-German Tech Misfire," Politico, November 17, 2025, https://www.politico.eu/article/anatomy-franco-german-tech-misfire-american-dependence/.

60 Draghi, "The Future of European Competitiveness," 34.

61 "President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations for Reauthorization," White House, July 2023, 3, https://int.nyt.com/data/documenttools/presidents-intelligence-advisory-board-and-intelligence-oversight-board-review-of-fisa-section-702-and-recommendations-for-reauthorization/4d2d32-18303fc702/full.pdf.

The United States has concluded CLOUD Act agreements with the United Kingdom (UK) and Australia, and negotiations are under way with Canada, all of which are members of the Five Eyes intelligence collective.[62] The UK agreement, the first to be concluded, has had a positive effect for that country's law enforcement agencies.[63] According to the US Department of Justice, UK agencies have already made more than twenty thousand direct requests to companies holding electronic evidence in the United States, including many for real-time interception of communications.[64] The results "provided UK Law Enforcement and Intelligence Agencies with critical data to tackle the most serious crimes facing UK citizens including terrorism; child sexual exploitation; drug trafficking; and organised crime," a UK government minister said in late 2023.[65]

Prosecutors from EU member states have looked across the channel jealously as their UK counterparts have made use of this powerful new investigative tool. In 2019, the EU authorized negotiation of an e-evidence agreement with the United States.[66] Talks began in earnest after the EU finalized its controversial counterpart to the CLOUD Act, the 2023 E-Evidence Regulation.[67] Progress has been slow and painstaking. In June 2024, senior EU and US home affairs and justice officials issued an optimistic joint statement welcoming "further progress" in the negotiations and looking "forward to advancing and completing" them.[68]

The Trump administration has paused EU-US negotiations without explanation. It might have concluded that CLOUD

Figure 4: US Cloud Act International Agreements

Source: US Department of Justice

Act agreements operate overwhelmingly to the advantage of foreign partners—the inevitable consequence of most relevant data being housed on servers located in the United States. As the Trump administration has demonstrated in

62 "Landmark U.S.-UK Data Access Agreement Enters into Force," US Department of Justice, press release, October 3, 2022, https://www.justice.gov/archives/opa/pr/landmark-us-uk-data-access-agreement-enters-force; "United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime," US Department of Justice, press release, December 15, 2021, https://www.justice.gov/archives/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime; "United States and Canada Welcome Negotiations of a CLOUD Act Agreement," US Department of Justice, press release, March 22, 2022, https://www.justice.gov/archives/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.

63 Robert Deedman and Kenneth Propp, "The U.K.-US Data Access Agreement," Lawfare, June 20, 2025, https://www.lawfaremedia.org/article/the-u.k.-u.s.-data-access-agreement.

64 "Report Concerning the Attorney General's Renewed Determination that the United Kingdom of Great Britain and Northern Ireland, and the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, Satisfy the Requirements of 18 USC. § 2523(B)," US Department of Justice, November 2024, https://www.documentcloud.org/documents/25551978-doj-report-to-congress-on-us-uk-cloud-act-agreement/.

65 Tom Tugendhat, "UK-US Data Access Agreement: First Year of Use," UK Parliament, December 19, 2023, https://questions-statements.parliament.uk/written-statements/detail/2023-12-19/hcws152?source=email.

66 "Recommendation for a Council Decision Authorizing the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters," European Commission, February 5, 2019, https://eur-lex.europa.eu/resource.html?uri=cellar:b1826bff-2939-11e9-8d04-01aa75ed71a1.0001.02/DOC_1&format=PDF.

67 "Council Adopts EU Laws on Better Access to Electronic Evidence," Council of the European Union, press release, June 27, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/.

68 "Joint Press Release Following the EU-US Ministerial on Justice and Home Affairs, 21 June 2024 (Brussels)," US Department of Homeland Security, June 28, 2024, https://www.dhs.gov/archive/news/2024/06/28/joint-press-release-following-eu-us-ministerial-justice-and-home-affairs-21-june.

trade negotiations with foreign countries, it is singularly focused on agreements that it can present as bringing more benefits for the United States. However, such a narrow focus overlooks other benefits of CLOUD Act agreements—sparing cloud providers conflicts of law, deterring data localization measures, and reducing the burden on the mutual legal assistance process.

In mid-2025, the UK government added an element of controversy to the use of CLOUD agreements by allegedly serving a request to Apple that it globally disable security features on its products.[69] If the UK successfully required Apple to remove security from a product (for example, by building in a backdoor to data that would otherwise be end-to-end encrypted), it could then use the CLOUD Act agreement to request the now-vulnerable data directly from the company. Apple challenged the request in a UK administrative court proceeding and issued a public statement warning customers about the measure's impact.[70] In addition, the White House and Congress sharply criticized the reported UK measure.[71] In August, the UK government withdrew its demand for access to Apple US customers' encrypted data, effectively conceding to the US objection.[72] It recently confirmed that the order had been reissued to apply only to UK users.[73] The US government could well demand that any EU e-evidence agreement include a similar commitment safeguarding US persons' data from surveillance by member states' authorities.

A US-EU e-evidence agreement would be an important advance in calming Europe's sovereign sensitivities about how US law enforcement authorities collect foreign-located evidence, just as the Data Privacy Framework has at least temporarily allayed Europe's concerns about US national security agencies' collection practices. Taken together, the two agreements would neutralize much of the political tension that has prevailed in these realms for more than a decade.

69 Richard Salgado and Kenneth Propp, "Patching the U.K.'s Zero-Day Saecurity Exploit With the US-U.K. CLOUD Act Agreement," Lawfare, July 31, 2025, https://www.lawfaremedia.org/article/patching-the-u.k.-s-zero-day-security-exploit-with-the-u.s.-u.k.-cloud-act-agreement.

70 Zoe Kleinman, "UK Demands Access to Apple Users' Encrypted Data," BBC, February 7, 2025, https://www.bbc.com/news/articles/c20g288yldko; "Apple Can No Longer Offer Advanced Data Protection the United Kingdom to New Users," Apple, September 23, 2025, https://support.apple.com/en-gb/122234.

71 Deedman and Propp, "The U.K.-US Data Access Agreement."

72 Annabelle Timsit and Joseph Menn, "U.K. Drops 'Back Door' Demand for Apple User Data, US Intel Chief Says," *Washington Post*, August 19, 2025, https://www.washingtonpost.com/technology/2025/08/19/uk-apple-backdoor-data-privacy-gabbard.

73 Christophe Domec, "Home Office Orders Apple to Allow Access to UK Users' Data," *Times*, October 2, 2025, https://www.thetimes.com/uk/technology-uk/article/home-office-orders-apple-to-allow-access-to-uk-users-data-tn3wlmhxq?gaa_at=eafs&gaa_n=AWEtsqdsuklSl3YWsv-OUFyP7S089T8e9EKaG--AY8onCxlbZei75ihDzjEfC_udtDU%3D&gaa_ts=695c0a2c&gaa_sig=35Ar1X-p304ize5_GRX2Gw4XVlD1VwyhVrWph_ApqbvZ53m8PgSK_1S27vfEYkfYMBS0EYM8CP22z5g-1iGUY4Q%3D%3D .

The US u-turn on data flows

After decades of the United States propounding unrestricted international commercial data flows—and bemoaning Europe's privacy impediments to them—the Biden administration made a dramatic course correction in late 2023.[74] Through parallel legislation (the Protecting Americans from Foreign Adversary Controlled Applications Act) and executive action, it imposed controls on certain categories of data exports to China, Russia, and other "foreign adversaries" citing national security reasons.[75] Subsequently, the Department of Justice issued a final rule and guidance to companies on compliance and enforcement.[76] Both the legislation and regulatory actions were spurred by reports that data brokers were collecting publicly available bulk data on US persons and selling them to foreign governments, which could enable them to—among other things—track the location of US military personnel.[77]

In addition to enacting domestic measures to limit certain international commercial data flows, the United States reversed course internationally. In the fall of 2023, the Office of the US Trade Representative withdrew its proposal to include in the Joint Statement Initiative on Electronic Commerce (JSI)—a World Trade Organization negotiation—a guarantee of the free flow of data across borders.[78] The final text of the JSI, announced in July 2024, not only lacks such an obligation but allows parties essentially unlimited scope to restrict data flows for data protection reasons, precisely as the EU had sought.[79] Even with these changes, the United States declined to join the JSI because it regarded the agreement's national security exception as insufficiently flexible, a move that some European Commission officials found puzzling.[80]

In contrast to the United States—and despite its long history of controlling data exports through the GDPR—the EU has moved slowly to evaluate the risks of data transfers to authoritarian states such as China and Russia. In 2021, the European Data Protection Board commissioned an outside report from academics that confirmed both countries' governments have access to individuals' personal information without commensurate rule-of-law protections, but it took no further action.[81] Even Russia's full-scale invasion of Ukraine has not served to entirely staunch the flow of European data to Russia. The Finnish and Dutch data protection authorities investigated data transfers by Yango, a subsidiary of the Russian search engine Yandex, but have not yet imposed restrictions.[82]

The past year, however, has seen a gradual shift in European regulators' thinking regarding data transfers to China. In May 2025, the Irish Data Protection Commission (DPC) fined TikTok €530 million after discovering it was transferring data to Chi-

74 Kenneth Propp, "Transatlantic Digital Trade Protections: From TTIP to 'Policy Suicide?'" Lawfare, February 16, 2024, https://www.lawfaremedia.org/article/transatlantic-digital-trade-protections-from-ttip-to-policy-suicide.

75 "Protecting Americans from Foreign Adversary Controlled Applications Act," in emergency supplemental appropriations, Pub. L. No. 118–50, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/7520/text; "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," White House, February 28, 2024, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

76 "Fact Sheet: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons," US Department of Justice, December 27, 2024, https://www.justice.gov/archives/opa/media/1382526/dl; "Data Security Program: Compliance Guide," US Department of Justice, April 11, 2025, https://www.justice.gov/opa/media/1396356/dl.

77 Justin Sherman, et al., "Data Brokers and the Sale of Data on US Military Personnel: Risks to Privacy, Safety, and National Security," Duke Sanford Tech Policy Program, November 2023, https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

78 Propp, "Transatlantic Digital Trade Protections."

79 "Joint Statement Initiative on Electronic Commerce," World Trade Organization, July 26, 2024, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True.

80 Kenneth Propp, "Who's a National Security Risk? The Changing Transatlantic Geopolitics of Data Transfers," Atlantic Council, May 29, 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/05/Whos-a-National-Security-Risk-The-Changing-Transatlantic-Geopolitics-of-Data-Transfers_Final.pdf.

81 "Government Access to Data in Third Countries: Final Report," Milieu Consulting, November 2021, https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

82 "The Data Protection Ombudsman's Decision Does Not Address the Legality of Data Transfers to Russia—the Matter Remains under Investigation," Office of the Data Protection Ombudsman, September 27, 2023, https://tietosuoja.fi/en/-/the-data-protection-ombudsman-s-decision-does-not-address-the-legality-of-data-transfers-to-russia-the-matter-remains-under-investigation#:~:text=The%20Office%20of%20the%20Data%20Protection%20Ombudsman%27s%20decision,Protection%.

na without requisite data protection safeguards.[83] In July, the DPC broadened its TikTok inquiry into whether the Chinese government could access such data when they are stored in China.[84] The Finnish data protection authority began a separate investigation into possible Chinese government access to health data that a Finnish university had shared with a Chinese genetic analysis company.[85]

Even Schrems, who has long challenged European data transfers to the United States, has turned his attention to China. Early in 2025, he filed complaints with European data protection authorities against six major Chinese consumer companies, including Shein, Temu, and WeChat, alleging government access to Europeans' personal data by an "authoritarian surveillance state."[86]

Recent moves by European data protection authorities to question whether China's government has impermissible access to Europeans' personal information mirror the rise in geopolitical tensions between Brussels and Beijing. Ireland's inquiry into TikTok data transfers, for example, can be read as asserting European data sovereignty against a geopolitical rival. The data dynamics are, in effect, a microcosm of Europe's larger dilemma with China—deep commercial dependency, but also a recognition that a degree of sovereign control is needed.

A single European data market

Brussels has recently expanded its laws promoting the secondary use of data for commercial, research, and government purposes, in hopes that these innovative legal measures will give homegrown companies a much-needed advantage in competing with data-rich foreign tech giants. However, the transfer of such data to non-EU companies has raised concerns about potentially protectionist restrictions. The Data Governance Act, the Data Act, and the European Health Data Space regulation—all enacted during the first von der Leyen commission—seek to stimulate a market for the secondary use of European data for commercial purposes.[87] These measures are based on the recognition that data collected by—and locked within—governmental or commercial organizations can have societal and economic benefits if made available for reuse by other entities.

The 2022 Data Governance Act grew out of a post-pandemic recognition of the potential for reuse of government-held data. It facilitates reuse by the private sector, for both commercial and non-commercial purposes, of government-held data (G2B), including data originally collected by public health, environmental, and transport authorities. Then Commissioner Thierry Breton hailed it as a step toward "an open yet sovereign European Single Market for data."[88]

83 "Irish Data Protection Commission Fines TikTok €530 Million and Orders Corrective Measures Following Inquiry into Transfers of EEA User Data to China," Data Protection Commission of Ireland, May 2, 2025, https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following.

84 "DPC Announces Inquiry into TikTok Technology Limited's Transfers of EEA Users' Personal Data to Servers Located in China," Data Protection Commission of Ireland, July 10, 2025, https://www.dataprotection.ie/en/news-media/press-releases/dpc-announces-inquiry-tiktok-technology-limiteds-transfers-eea-users-personal-data-servers-located.

85 Kristof Van Quathem and Anna Sophia Oberschelp de Meneses, "Finnish Supervisory Authority Investigates Health Data Transfers to China," Covington, March 19, 2025, https://www.insideprivacy.com/cross-border-transfers/finnish-supervisory-authority-investigates-health-data-transfers-to-china/.

86 "TikTok, AliExpress, SHEIN & Co Surrender Europeans' Data to Authoritarian China," Noyb, January 16, 2025, https://noyb.eu/en/tiktok-aliexpress-shein-co-surrender-europeans-data-authoritarian-china.

87 "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act)," *Official Journal of the European Union*, May 30, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868; "Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)," *Official Journal of the European Union*, December 13, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854; "Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and Amending Directive 2011/24/EU and Regulation (EU) 2024/2847," *Official Journal of the European Union*, February 11, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500327.

88 "Commission Proposes Measures to Boost Data Sharing and Support European Data Spaces," European Commission, press release, November 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102.

The Data Governance Act was followed a year later by the even more ambitious Data Act, which concentrated on expanding business-to-business sharing of non-personal data, such as the industrial data generated by connected devices. The Data Act sought to ease legal issues that arise with reuse by third parties, such as intellectual property protection and trade secret rules. Both laws insisted upon additional safeguards for transferring data to companies in third countries, such as the United States, where that data could become subject to governmental access. The European Commission further envisaged a series of sector-specific European data spaces, each requiring separate legislation.[89] They would cover sectors—from agriculture to energy to transportation—that generate large amounts of industrial data ripe for reuse. The European Health Data Space regulation is the first of this series to be enacted.

At the start of the current commission mandate, von der Leyen's mission letter to Virkkunen instructed her to deepen focus on the reuse of data. She was asked to "present a European Data Union Strategy drawing on existing data rules to ensure a simplified, clear and coherent legal framework for businesses and administrations to share data seamlessly and at scale, while respecting high privacy and security standards."[90] The commission duly launched a public consultation process, articulating as its aim "expanding the availability and use of data to support AI development."[91] Published on November 19, 2025, the Data Union Strategy seeks to safeguard the EU's data sovereignty by ensuring fair conditions for cross border flows of non-personal data; "linking EU data ecosystems with those of like-minded partners;" and "boosting the EU voice in global data governance."[92] This is intended to build a comprehensive legal regime for secondary data access that will enable European industry to catch up with the US tech giants that already enjoy access to vast pools of proprietary data.

EU content moderation and free speech

One of the EU's proudest recent legislative accomplishments is the 2023 Digital Services Act, a sprawling and complex framework regulating online platforms' accountability for illegal content, including illegal hate speech.[93] It imposes the most onerous requirements on very large online platforms, half of which are US companies. The Trump administration and the Republican-led Congress have sharply criticized the DSA, viewing it as a tool for the suppression of right-wing populist political speech.[94] On the contrary, the EU views certain DSA provisions, such as transparency tools and safeguards against arbitrary content moderation, as intended to protect free speech.

Trump singled out the DSA for criticism in the February 2025 official memorandum on preventing the "Unfair Exploitation of American Innovation," while the Republican chair of the Federal Communications Commission called it "incompatible with both our free speech tradition in America and the commitments that these technology companies have made to a diversity of opinions."[95] The US State Department began a di-

89 "Common European Data Spaces," European Commission, October 27, 2025, https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

90 "Mission Letter: Henna Virkkunen, Executive Vice-President-Designate for Tech Sovereignty, Security and Democracy," European Commission, September 17, 2024, https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b-7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf.

91 "Public Consultation on the Use of Data to Develop the Future of AI: The European Data Union Strategy," European Data, June 25, 2025, https://data.europa.eu/en/news-events/news/public-consultation-use-data-develop-future-ai-european-data-union-strategy.

92 "Communication from the Commission to the European Parliament and the Council: Data Union Strategy: Unlocking Data for AI," European Commission, November 19, 2025. https://digital-strategy.ec.europa.eu/en/policies/data-union.

93 "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)," *Official Journal of the European Union*, October 27, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.

94 Jeanna Smialek and Adam Satariano, "Something Else for Europe and the US to Disagree About: 'Free Speech,'" *New York Times*, April 4, 2025, https://www.nytimes.com/2025/04/04/world/europe/european-union-free-speech-x-facebook-elon-musk.html.

95 "Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation"; Supantha Mukherjee, "US FCC Chair Says EU Digital Services Act Is Threat to Free Speech," Reuters, March 3, 2025, https://www.reuters.com/technology/eu-content-law-incompatible-with-us-free-speech-tradition-says-fccs-carr-2025-03-03/.

Reform UK party leader Nigel Farage before a House Judiciary Committee hearing entitled "Europe's threats to American speech and innovation" in Washington, DC, September 3, 2025. Source: REUTERS/Nathan Howard.

plomatic campaign, alleging, "In Europe, thousands are being convicted for the crime of criticizing their own governments."[96] A leaked August 2025 cable to European posts directed US diplomats to advocate for a narrowing of the DSA's definition of illegal content, among other ambitions. The European Commission firmly pushed back, describing the censorship allegations as "completely unfounded" and insisting that its digital legislation "will not be changed."[97]

The Republican majority on the House of Representatives Judiciary Committee also weighed in with a strongly worded staff report describing the DSA as an "anti-speech, Big Brother law."[98] The report identified a handful of examples of how the act could function to restrict speech extraterritorially. For example, in an August 2024 letter, then Commissioner Breton warned Elon Musk's X platform that the effects of a campaign interview it hosted with Trump could spill over into the EU

96 Department of State (@StateDept), "In Europe, thousands are being convicted for the crime of criticizing their own governments. This Orwellian message won't fool the United States. Censorship is not freedom," X post, July 22, 2025, https://x.com/statedept/status/1947755665520304253.

97 Humeyra Pamuk, "Rubio Orders US Diplomats to Launch Lobbying Blitz against Europe's Tech Law," Reuters, August 7, 2025, https://www.reuters.com/sustainability/society-equity/rubio-orders-us-diplomats-launch-lobbying-blitz-against-europes-tech-law-2025-08-07.

98 "The Foreign Censorship Threat: How the European Union's Digital Services Act Compels Global Censorship and Infringes on American Free Speech," Committee on the Judiciary of the US House of Representatives, July 25, 2025, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2025-07/DSA_Report%26Appendix%2807.25.25%29.pdf.

and spur commission retaliatory measures under the DSA.[99] The committee also cited a request to X by the French national police that the platform remove a post originating from a US-based account suggesting France's immigration and citizenship policies were to blame for a 2023 terrorist attack a Syrian refugee committed in that country.[100]

The chairman of the US FTC launched a further salvo in August, warning US companies that their very compliance with the EU's DSA, or with the UK's similar Online Services Act or its surveillance authorities, could constitute a violation of the FTC Act, which prohibits unfair or deceptive commercial acts or practices. FTC Chairman Andrew N. Ferguson suggested, "It might be an unfair practice to subject American consumers to censorship by a foreign power by applying foreign legal requirements, demands, or expected demands to consumers outside of that foreign jurisdiction."[101]

This transatlantic dispute over the DSA and similar content moderation laws reflects differing US and European historical traditions on speech regulation.[102] The US Supreme Court has identified only speech creating a "clear and present danger" of inciting violence or other illegal conduct as suitable for restriction. Many European judiciaries, informed by their countries' twentieth century histories of hate speech, take a more cautious view. For example, Germany bans speech glorifying or denying the Holocaust, while Denmark makes it illegal to burn the Quran. The DSA is the EU's attempt to ensure that platforms remove content deemed illegal, both offline and online, but the act's lack of definitions leaves a door open to abuse.

On December 23, 2025, the Trump administration raised the stakes in its free speech campaign against European content moderation laws. Secretary of State Marco Rubio issued determinations under the Immigration and Nationality Act barring from entry into the United States five Europeans associated with content moderation.[103] The headliner was Thierry Breton, an architect of the DSA; the others hail from European non-governmental organizations that track hate speech and disinformation on the internet. The European Commission quickly issued a statement that it "strongly condemns" the US actions, reiterating its "sovereign right to regulate economic activity in line with our democratic values."[104] As the Trump administration continues its ideological campaign against the DSA, the transatlantic dispute over free speech seems bound to escalate.

Cybersecurity and cloud services

In 2022, the European Union Agency for Cybersecurity (ENISA) began an effort to harmonize member-state cybersecurity requirements for government data processing contracts. The European Commission averred that cloud services were a "strategic dependency" on a handful of large providers headquartered in the United States.[105] Several EU member states, led by France, argued for including sovereignty requirements in the envisaged EU Cybersecurity Scheme (EUCS).

A leaked 2023 ENISA draft proposed that the EU impose sovereignty requirements similar to those in France's domestic security certification and labeling program, SecNumCloud, for contracts involving the most sensitive government data. SecNumCloud has an announced goal that, in order to obtain a trust certificate, cloud service providers must be "immune to any extra-EU regulation."[106] ENISA proposed incorporating this requirement into EU law as well, adding restrictions on foreign

99 Mark Scott, "EU Takes Shot at Musk over Trump Interview—and Misses," *Politico*, August 13, 2024, https://www.politico.eu/article/eu-elon-musk-donald-trump-interview-thierry-breton-letter-social-media/.

100 "The Foreign Censorship Threat."

101 "Model Letter sent to Tech Companies from Chairman Andrew N. Ferguson," US Federal Trade Commission, August 21, 2025, https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-unfair-security-letter-ferguson.pdf.

102 Propp, "Talking Past Each Other."

103 "Announcement of Actions to Combat the Global Censorship-Industrial Complex," US Department of State, press release, December 23, 2025, https://www.state.gov/releases/office-of-the-spokesperson/2025/12/announcement-of-actions-to-combat-the-global-censorship-industrial-complex/.

104 "Statement by the European Commission on the U.S. Decision to impose travel restrictions on certain EU individuals," European Commission, press release, December 23, 2025, https://ec.europa.eu/commission/presscorner/detail/en/statement_25_3160.

105 "EU Strategic Dependencies and Capacities: Second Stage of In-Depth Reviews," European Commission, February 22, 2022, https://www.wec-italia.org/wp-content/uploads/2022/02/STRATEGIC-DEPENDENCIES-2022.pdf.

106 "Doctrine 'Cloud au Centre' sur l'Usage de l'Informatique en Nuage au Sein de l'État," Government of the Republic of France, July 5, 2021, https://www.transformation.gouv.fr/files/presse/Circulaire-n6282-SG-5072021-doctrineuutilisation-informatique-en-nuage-Etat.pdf.

ownership and insisting on localization of cloud services operations and data within the EU.

EU member states divided over whether to adopt such cybersecurity requirements, which could have the effect of disqualifying large foreign cloud service providers from sensitive government data processing contracts. In addition, some European companies, especially in the financial sector, argued that the foreign providers offered greater cybersecurity as well as a superior technical product.[107] The Office of the US Trade Representative formally questioned whether the potential EUCS restrictions were consistent with the EU's obligations under the World Trade Organization's Government Procurement Agreement (GPA).[108]

In 2024, the Belgian EU presidency put forward a compromise proposal that discarded the foreign ownership restrictions in favor of data labeling and localization requirements.[109] French authorities and technology companies expressed dismay at the prospect of EU-level cybersecurity certification rules weaker than France's own.[110] ENISA has yet to issue the final implementing measure, and this debate could well reemerge in the context of the anticipated CADA.

Looking ahead: Transatlantic tension will persist

The European debate over digital sovereignty—now firmly linked to the wider debate over technological sovereignty—is likely to be a continuing point of tension in the US-EU relationship. For many years, this has been a rhetorical exercise with few real consequences for non-EU firms, especially US companies. But the shift in geopolitics and the increasing drive to support EU industries to build a more competitive economy have led many European policymakers to conclude that now is the time to act. Moreover, the geopolitics are not just about Russia's aggression or China's export domination. They are also about the shifts and inconsistencies in US policy that have made many in Europe believe that it must now begin to fend for itself, in terms of both defense and the economy.

As a result, the debate over digital sovereignty has moved from a discussion of whether there should be limits on non-EU companies to a discussion of how many restrictions there will be, and of what type and in what sectors of the economy. That discussion is likely to be pursued through several key legislative initiatives planned for late 2025 and 2026. CADA is already expected to identify requirements—including sovereign requirements—for cloud services.

Perhaps most relevant, the public procurement directives are already under internal review, with a proposal for revision expected from the commission in 2026.[111] Because much of the debate is about who can sell which products and services to whom (including to governments), procurement policy will be a key instrument in imposing sovereign requirements. EU and member-state procurement rules currently privilege price as the key selection criteria but, in the Net Zero Industry Act and other new measures, other considerations have been introduced into the procurement calculation.

As the EU pursues these initiatives, it will face a dilemma: To what degree does sovereignty require autarky? Or does the EU require partnerships, despite the risk of dependencies, because of the current lack of key capabilities? Some in Europe have argued that the right way forward is to develop end-to-end EU capabilities in the form of a Eurostack.[112] From

107 Laura Kabelka, "Sovereignty Requirements Remain in Cloud Certification Scheme Despite Backlash," Euractiv, July 16, 2022, https://www.euractiv.com/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash.

108 "2024 National Trade Estimate Report on Foreign Trade Barriers," Office of the US Trade Representative, March 2024, https://ustr.gov/sites/default/files/2024%20NTE%20Report_1.pdf.

109 Floris Hulshoff Pol, "EU Drops Sovereignty Rules for US Cloud Providers," Techzine, April 4, 2024, https://www.techzine.eu/news/privacy-compliance/118401/eu-drops-sovereignty-rules-for-u-s-cloud-providers/.

110 Reynald Fléchaux, "EUCS, la Certification Cloud Européenne qui Menace de Désarmer SecNumCloud," CIO, September 12, 2024, https://www.cio-online.com/actualites/lire-eucs-la-certification-cloud-europeenne-qui-menace-de-desarmer-secnumcloud-15856.html.

111 Francesco Nicoli, "Mapping the Road Ahead for EU Public Procurement Reform," Bruegel, March 21, 2025, https://www.bruegel.org/first-glance/mapping-road-ahead-eu-public-procurement-reform.

112 Théophane Hartmann, "European Industry Big Win: Germany, France Both Support Sovereign EU-Based Tech Infrastructure," Euractiv, April 10, 2025, https://www.euractiv.com/news/european-industry-big-win-germany-france-both-support-sovereign-eu-based-tech-infrastructure/.

fiber-optic networks and computing hardware to software development and cybersecurity capabilities, all would be provided by EU companies.[113] Others have pointed to the difficulties with this, asking whether the lack of EU-owned capabilities in cloud, AI, search, and other key functions would doom such an effort to be inferior and thus push Europe farther behind in the race to innovate essential digital technologies for the future. They also fear that European companies will not be able to compete internationally if they are cushioned by sovereign requirements.[114] Some see no contradiction between sovereignty and being open to non-EU firms; indeed, they see access to the most innovative global companies as essential, especially given Europe's competitiveness challenge.[115] For others, the key element is timing. The EU tech sector currently lags in innovation but, with proper support and time, it should be fully capable of growing world-leading firms and technologies.[116] Indeed, the EU's International Digital Strategy emphasizes the importance of partners in boosting EU competitiveness and innovation, and the EU's ambitions in global governance for data can hardly be accomplished without cooperative partners.[117]

But in all these versions of digital sovereignty, as well as in the larger arena of tech sovereignty, there is a central question: who owns the companies involved, and does it matter if they are not EU firms as long as they abide by EU laws and regulations? The recent negotiations over an EU-wide cloud certification system stalled on exactly this point (see the above discussion of EUCS). The Toolbox for 5G Cybersecurity put forward the concept of a "high-risk supplier" to warn against non-EU companies that were insufficiently independent of their home governments. While this was aimed at Chinese companies—especially Huawei—concerns have more recently focused on the United States and its companies.

The EU's concerns are not only about the dominant position of US platforms in the European digital market, but also the potential actions of the US government—especially the Trump administration. The administration's inconsistency on Ukraine, highlighted by its threats in July 2025 to cease sending weapons and other military supplies to Ukraine (reversed shortly after), alarmed many in Europe.[118] Reports that the Trump administration threatened to block Ukraine's access to the vital communications network Starlink during negotiations over critical minerals also raised European concerns.[119] While these instances were primarily about defense, not the digital arena, they have created a heightened sense of insecurity in Europe. Coupled with the experience of the trade negotiations, they put into question the reliability of the United States as a partner in any undertaking.

In this environment, the EU will need to make choices about how best to ensure it has sufficient sovereignty over its digital market. Will the answer be found in more restrictions on non-EU companies, or with a more open arrangement that also boosts European economic growth and competitiveness?

113 Michal Kobosko, "A European Recipe for Tech Sovereignty," *Parliament*, July 30, 2025, https://www.theparliamentmagazine.eu/news/article/oped-a-european-recipe-for-tech-sovereignty.

114 For a detailed discussion of the challenges facing Eurostack and the more exclusionary version of EU digital sovereignty, see: Zach Meyers, "Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?" Centre on Regulation in Europe, September 2025, https://cerre.eu/wp-content/uploads/2025/09/CERRE_Issue-Paper_EU-Competitiveness_Can-the-EU-reconcile-digital-sovereignty-and-economic-competitiveness.pdf.

115 "Clearing the Cloud," Implement Consulting Group in collaboration with Google, November 2025, https://cms.implementconsultinggroup.com/media/uploads/articles/2025/European-digital-sovereignty/2025-Clearing-the-cloud.pdf.

116 See, for example: "Open Letter: European Industry Calls for Strong Commitment to Sovereign Digital Infrastructure," Euro-Stack, March 14, 2025, https://euro-stackletter.eu/wp-content/uploads/2025/03/EuroStack_Initiative_Letter_14-March-.pdf. The letter, signed by numerous European companies, argues for increased support to European industry to build a Eurostack, while not restricting access by non-EU companies.

117 "Joint Communication on an International Digital Strategy for the EU," European Commission and EU High Representative for Foreign and Security Policy, June 5, 2025, https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu.

118 Amy Mackinnon, Jamie Dettmer, and Paul McLeary, "Europe Scrambles to Aid Ukraine after US Intelligence Cutoff," *Politico*, March 8, 2025, https://www.politico.com/news/2025/03/08/europe-scrambles-to-aid-ukraine-after-us-intelligence-cutoff-00219678.

119 Andrea Shalal and Joey Roulette, "US Could Cut Ukraine's Access to Starlink Internet Services over Minerals, Say Sources," Reuters, February 22, 2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

Seven recommendations for Brussels and Washington

Given the economic stakes involved for both parties, the EU should engage the United States as it moves forward, and should keep the following guidelines in mind.

Competitiveness is key to innovation and economic success. Throughout the coming debates over sovereign requirements, the EU must balance the need for security and for its own industrial and digital capabilities with the efficiencies and productivity required for a globally competitive economy. Settling for a more expensive and less capable product or service because it is European owned is not the way to grow the economy. There are times when it is necessary, but these instances should be rare and well considered, not routine.[120]

Heated rhetoric on either side does not help the economy. As the EU moves forward with legislation, both Washington and Brussels should seek to lower the temperature. While some US executive orders and statements from top officials have seemed to decry any EU regulation that impedes US companies, the reality is that Europe has the right to regulate as it sees fit in its own market, as does the United States. At the same time, European threats of broad sovereign restrictions do not encourage needed investment. It should not be forgotten that the US-EU trade and investment relationship is the largest such partnership in the world, worth around $1.5 trillion in goods and services trade in 2024, and with mutual investment worth several times that.[121] As both parties establish regulatory or investment requirements intended to boost domestic capabilities and add resilience to their economies, there will inevitably be tensions and misunderstandings. Creating barriers to trade and investment is sometimes necessary in limited circumstances, but careful consultations can ameliorate their impact.

Agreed legal frameworks in key areas can ease the need for sovereign protections. As the discussion of data policy demonstrates, the transatlantic economy is not just about products and services, but also the data generated by them. Sharing those data—and being able to use them to generate revenues—is key to success in the digital economy. Of course, those transferring and using data must comply with local laws, including the GDPR. But the US and EU regulatory regimes collide at times, offering inconsistent or even conflicting requirements. Negotiated arrangements, such as the US-EU Data Privacy Framework, can overcome those differences and provide a stable context for business. A US–EU agreement on law enforcement access to data likewise could provide the protections and access both parties need. Similarly, an agreement that facilitates transfers of non-personal data might be useful in response to the Data Act and Data Union Strategy. Now is the time to make sure the United States and EU are developing compatible regimes.

Ringfencing can be a valuable strategy, as can trusted vendors. Not all suppliers and customers are equal. Arrangements among allies and partners can lessen risks while preserving as much of the open, prosperous economy as possible, even in sensitive sectors. It makes no sense for Europeans to focus more on the transfer of data to the United States than to Russia or China. Using criteria such as those in the EU Toolbox for 5G Cybersecurity to identify foreign companies that can partner in key sectors will provide clarity and ease transactions. Similarly, a proposal floated in the EUCS negotiations that the trusted circle of cybersecurity providers be based on NATO membership might be appropriate. The Group of Seven (G7) could also offer a starting point for developing a set of compatible, interacting regulatory regimes in the digital economy, as it has done to some degree through its discussion of data free flow with trust and the AI principles and code of conduct.[122]

Certain sectors of the economy are more sensitive than others. Digital sovereignty requirements should not be imposed on broad swaths of the economy. There are two main reasons for such requirements: national security and creating an indigenous capability in those areas where national economic resiliency is required. Policymakers should carefully identify the areas of the economy where these two reasons apply. Cybersecurity for essential government operations and protecting critical infrastructure are good examples. Management of more prosaic, but still sensitive government data—including where they are stored and who has access—might not need such stringent requirements. Because digital elements—data, cloud, software, and increasingly AI—exist across the economy, it might be more helpful to think about specific functions and make a risk-based assessment of the consequences

120 For a discussion of the relationship between digital sovereignty and competitiveness, see: Christian Klein, "The Boss of SAP on Europe's Botched Approach to Digital Sovereignty: It's Time to Prioritise Code over Concrete," Economist, August 25, 2025, https://www.economist.com/by-invitation/2025/08/25/the-boss-of-sap-on-europes-botched-approach-to-digital-sovereignty.

121 "European Union," Office of the United States Trade Representative, last visited December 11, 2025, https://ustr.gov/countries-regions/europe-middle-east/europe/european-union.

122 "G7 Roadmap for Cooperation on Data Free Flow with Trust," Group of Seven, 2021, https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf; "G7 Leaders' Statement on the Hiroshima AI Process," Group of Seven, October 30, 2023, https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process.

of failure. Sovereign requirements should be limited to those areas in which a failure or breach will have consequences across society and the economy.

The type of sovereign requirement can vary with the economic sector and even particular conditions. Among European policymakers, the sovereign requirements currently under discussion can be divided into two types: those that require a supplier to adhere to specific rules and those that involve restrictions relating to the ownership of the company supplying a particular service or product. The first might involve data localization or restricting access to data or use of a particular technology, such as AI. The second, which has been applied in the French SecNumCloud, is far more restrictive and affects the ability of any US-based company to provide the service in question. In some cases, an ownership restriction might exclude companies with the best capabilities from providing the service, and could even expose those using the service to more risk. Thus, ownership restrictions are unlikely to be worthwhile except in rare cases. In the United States, these exist in areas of defense contracting, in which companies dealing with US classified material must set up a US company with US governance and employees. But most government digital contracts, both in the United States and in Europe, are not defense related and would not require such far-reaching ownership rules.

Instead, for those functions in which a breach or disruption would cause significant harm, creating a category of trusted vendors might be appropriate. This could apply to sensitive government functions, as well as to critical infrastructure provided by private-sector enterprises. A system based on trusted vendors could balance the desire to boost local providers while also securing access to top-quality services from non-EU companies. The EU might consider whether there are lessons to be learned from the US government's FedRAMP system, which certifies companies (including non-US companies) to provide cloud services to different government customers. Companies need to meet criteria that become more restrictive and complex through the three levels of certification (low, moderate, and high).[123] While FedRAMP applies across most of the US government, individual agencies have the ability to impose their own requirements, allowing national security and intelligence agencies to impose further restrictions on those involved in classified functions. Despite these exceptions, FedRAMP's graduated approach—matching certification level to sensitivity of the data—is much more tailored than some European proposals in matching certification requirements to the risk level of the cloud service required.[124]

Sovereign requirements should be implemented in a consistent manner, including at the member-state level. One of the persistent challenges of EU policy is ensuring that implementation is the same throughout the union. Both the Draghi and Letta reports cited differences in member-state requirements for businesses (or implementation of those requirements) as a key factor slowing EU competitiveness. The US trade representative has cited as trade barriers numerous instances of different requirements among EU member states, meaning that companies must follow multiple sets of rules even within the single market.[125] The European Commission recognized this problem when it decided that, under the DSA, very large online platforms (VLOPs) should be regulated at the EU level, not by member-state authorities. As the EU develops sovereign requirements in the digital sphere, it should be alert to efforts by member states to toughen criteria in ways that add unwarranted restrictions.

While the EU certainly has the right to decide on its own digital sovereignty requirements, those measures will undoubtedly affect access of non-EU companies to the market as well as the capabilities that are accessible to the EU and its member states. There will be costs for the EU, especially as it tries to build a more competitive economy. For that reason, any restrictions should be focused on those circumstances in which risks are high and security is necessary. This exercise should not be about denying access to non-EU companies, but instead about building a secure digital environment and resilient European capabilities. The EU should engage with its partners—not only the United States, but also Japan, South Korea, the UK, and others—to ensure that the fewest possible frictions arise. This will be a test for the transatlantic relationship, but one that can lead to greater cooperation rather than continued angst.

123 For details on the FedRAMP program, see: "FedRAMP Provides a Standardized, Reusable Approach to Security Assessment and Authorization for Cloud Service Offerings," FedRAMP, last visited December 11, 2025, https://www.fedramp.gov.

124 For a discussion of the differences between FedRAMP and EUCS, see: Kenneth Propp, "Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services," Cross Border Data Forum, June 27, 2023, https://www.crossborderdataforum.org/wp-content/uploads/2023/07/Oceans-Apart-The-EU-and-US-Cybersecurity-Certification-Standards-for-Cloud-Services.pdf.

125 "2025 National Trade Estimate Report on Foreign Trade Barriers," Office of the US Trade Representative, 2025, https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf.

About the authors

Frances G. Burwell is a distinguished fellow at the Atlantic Council's Europe Center and a senior director at McLarty Associates. Until January 2017, she served as vice president, European Union and Special Initiatives, at the Council. She has served as director of the Council's Program on Transatlantic Relations, and as interim director of the Global Business and Economics Program, and currently directs the Transatlantic Digital Marketplace Initiative. Her work focuses on the European Union and US-EU relations as well as a range of transatlantic economic, political, and defense issues. She is a member of the Advisory Board of Allied for Startups.

Her most recent report is The art of the transatlantic deal. Her other publications include Digital sovereignty in practice: The EU's push to shape the new global economy; The US-EU Trade and Technology Council: Assessing the record on data and technology issues; Engaging Europe: A Transatlantic Digital Agenda for the Biden Administration; The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? (co-authored); Making America First in the Digital Economy: The Case for Engaging Europe (2018); After Brexit: Alternate Forms of Brexit and their Implications (co-authored); Europe in 2022: Alternative Futures (co-authored with Mathew Burrows); A Transatlantic Approach to Europe's East: Relaunching the Eastern Partnership; Shoulder to Shoulder: Forging a Strategic US-EU Partnership; Rethinking the Russia Reset; and Transatlantic Leadership for a New Global Economy. She is also a frequent commentator on European politics and transatlantic relations, with interviews and op-eds appearing in the Huffington Post, Handelsblatt Global Edition, Financial Times, al-Jazeera, BBC, National Public Radio, CNBC, CCTV, among others.

Kenneth Propp is a nonresident senior fellow with the Atlantic Council's Europe Center. He is also an adjunct professor of European Union Law at the Georgetown University Law Center and a senior fellow with the Cross-Border Data Forum. He advises and advocates on data trade, privacy, security, and other regulatory issues in the United States and major international markets. From 2011 to 2015, he served as legal counselor at the US Mission to the European Union (EU) in Brussels where he led US government engagement on privacy law and policy and digital regulation, and advised on trade negotiations with the EU. In previous assignments for the Office of the Legal Adviser at the US Department of State, Propp specialized in legal issues relating to international criminal law and international trade and investment law. He also served as legal adviser to the US embassy in Germany. Propp holds a JD from Harvard Law School and a bachelor's degree from Amherst College.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005