Atlantic Council

EUROPE CENTER

Digital Sovereignty in Practice:

The EU's Push to Shape the New Global Economy

By Frances G. Burwell and Kenneth Propp

Europe Center

The Europe Center conducts research and uses real-time commentary and analysis to guide the actions and strategy of key transatlantic decisionmakers on the issues that will shape the future of the transatlantic relationship and convenes US and European leaders through public events and workshops to promote dialogue and to bolster the transatlantic partnership.

The Atlantic Council'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.

Atlantic Council

EUROPE CENTER

Digital Sovereignty in Practice:

The EU's Push to Shape the New Global Economy

By Frances G. Burwell and Kenneth Propp

ISBN-13: 978-1-61977-254-0

Cover: European Commission President Ursula von der Leyen delivers the State of the European Union address to the European Parliament, in Strasbourg, France. September 14, 2022. REUTERS/Yves Herman.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

October 2022

Contents

Executive Summary

Since Ursula von der Leyen became European Commission president almost three years ago, there has been a sometimes-sharp transatlantic discussion about the impact of the European Union's push for "digital sovereignty." While that concept remains largely undefined, it nonetheless has informed a comprehensive set of legislative proposals that illustrate its key elements. The European Union (EU) intends to:

- provide significant support for development of EU-based technological capabilities;
- lead in the creation of global regulatory norms for the digital economy; and
- address concerns about the continent's vulnerability to external actors, including by limiting non-EU participation in some areas of the European market.

Since the advent of the von der Leyen commission in late 2019, the EU has adopted the Digital Markets Act and the Digital Services Act, both intended to regulate the behavior of online platforms. The Data Governance Act and the European Chips Act are intended to boost European innovation in key elements of the digital economy. The Artificial Intelligence Act and the Data Act are still in the legislative process, but expected to be finalized in 2023 and then regulate the use of artificial intelligence (AI) (especially high-risk AI) and the use and monetization of data among companies (see page sixteen for a list of EU initiatives). These legislative packages—and others—are supplemented by a variety of certifications and other regulatory requirements.

Every government has a right to regulate its own digital economy. But at this particular geopolitical moment, it is vital that Western democracies find ways to address the challenges of the digital economy together, and avoid creating rules that make such cooperation more difficult. Because the EU represents a major global market, its ambitions in the digital arena and its ability to cooperate with other likeminded democracies will be crucial to building a strong coalition against the authoritarian challenge.

The United States has several options for responding to discriminatory or protectionist aspects of EU digital sovereignty, including possibly invoking the World Trade Organization (WTO) dispute-settlement mechanism. But it would be more constructive if the EU and United States engaged in a full and frank discussion of such concerns within the confines of the new US-EU Trade and Technology Council (TTC). In particular, the TTC could provide a platform for building cooperation on research and innovation, and for coordinating US and EU approaches to international standards for emerging technologies. If this approach is to work, however, the EU must keep its own standards-development process open and inclusive, and it must resist measures that treat its allies in the same way as its "systemic rival," China. The United States, for its part, must better identify its own priorities for the digital economy. While the EU has led in regulating the digital economy, the United States has given few concrete indications of a systematic approach toward the challenges of digitalization.

Finally, it is time for the United States and EU to reach out to likeminded governments to build a coalition, ensuring that—in the face of authoritarianism—a common democratic approach on digital issues can reinforce an open global economy. This effort could build upon existing multilateral and plurilateral arrangements, including some put forward by the Group of Seven (G7) and the Organisation for Economic Co-operation and Development (OECD). It is time for the EU, the United States, and others to build the strong cooperation in the digital economy that the current geopolitical world requires.

The Search for Digital Sovereignty

Over the past three years, "digital sovereignty" has emerged as a priority ambition in European discussions regarding emerging technologies and digital policy. As European Commission President Ursula von der Leyen made clear in early remarks before the European Parliament, her goal was for Europe to achieve "technological sovereignty in some critical technology areas."[1] Since then, calls for the European Union (EU) to attain greater autonomy in digital technologies and policies have continued, notably in the commission's 2021 "Digital Compass," which called for the EU to "secure digital sovereignty" by developing key technologies, fostering digital skills, and boosting digitalization in key sectors.[2] Most importantly, the commission launched an extensive legislative agenda designed to support the use of key technologies, such as artificial intelligence (AI), quantum computing, and semiconductors, while also establishing rules for the management of digital activities, from content moderation and use of industrial data to market competition.

But what do European politicians mean by "digital sovereignty"? The EU model of digital sovereignty, as it has developed, has three elements, including:

- **significant support in terms of resources and policy for the development of indigenous EU capabilities in emerging technologies,** as well as for the broader digitalization of the European economy; through greater support for research, as well as industry, the EU plans to become a leader in areas such as cloud, quantum computing, and AI;

- **an explicit ambition to create global norms and "gold standards"** in the regulation and standardization of digital technologies, drawing on the experience of the General Data Protection Regulation (GDPR); and

- **rules at both the EU and member-state levels designed to reduce exposure to external decision-makers** (whether corporate or government) by restricting the access of non-EU actors to the EU market and limiting their scope of activity within it; for example, by controlling the transfer of European assets, such as data, from that market.

Executive Vice President of the European Commission for A Europe Fit for the Digital Age Margrethe Vestager speaks at a news conference on the 2030 Digital Compass in Brussels, Belgium. March 9, 2021. Olivier Hoslet/Pool via REUTERS.

When the von der Leyen commission came into office in 2019, it was unclear whether the call for digital sovereignty would go beyond rhetorical flourish. In our June 2020 report, we warned about the potential impact on transatlantic relations, but cautioned that many specifics of future European rules were still unclear.[3] But with the release and gradual adoption of key legislative proposals, as well as new national rules in some member states, a pattern has emerged: resources and regulations are aimed at supporting the "Europeanization" of key technologies and assets (including data). In a growing set of circumstances, non-EU companies, wherever they operate, must prove their ability

1 Mark Scott, "What's Driving Europe's New Aggressive Stance on Tech," *Politico,* October 27, 2019, https://www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen/.

2 "2030 Digital Compass: The European Way for the Digital Decade," European Commission, March 9, 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

3 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/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/.

to meet EU standards, with little distinction made between companies based in allied countries—including the United States—and those based in authoritarian states such as China. The tendency toward Europeanization has been accelerated by the search for greater resiliency in digital infrastructures and technologies, especially in the wake of the COVID-19 pandemic and the Russian invasion of Ukraine.

This is not the same form of digital sovereignty that is emerging in techno-authoritarian countries, including Russia, China, and even Turkey. Those governments sometimes cite EU rules to justify their own actions, but their motives are very different: they seek to use digital technologies to increase regime control over public debate, or to watch and restrict opposition groups. In contrast to that of the techno-authoritarians, the EU version of digital sovereignty does not give governments privileged access to technology and data, nor reinforce regime control over the digital economy. Rather, EU policymakers see it as intended to protect the interests of individuals and companies in the EU. But in seeking to promote a "sovereign" ability to safeguard those citizens and manage the European digital economy, the EU and its member states seem willing to use measures that veer toward discrimination and protectionism. At the very least, the EU's single-market power has the ability to shape standard setting around the world, and the EU has demonstrated a willingness to force others to adopt EU standards or forgo access to its market. In some cases, EU or member-state rules disqualify non-EU companies from a part of that market.

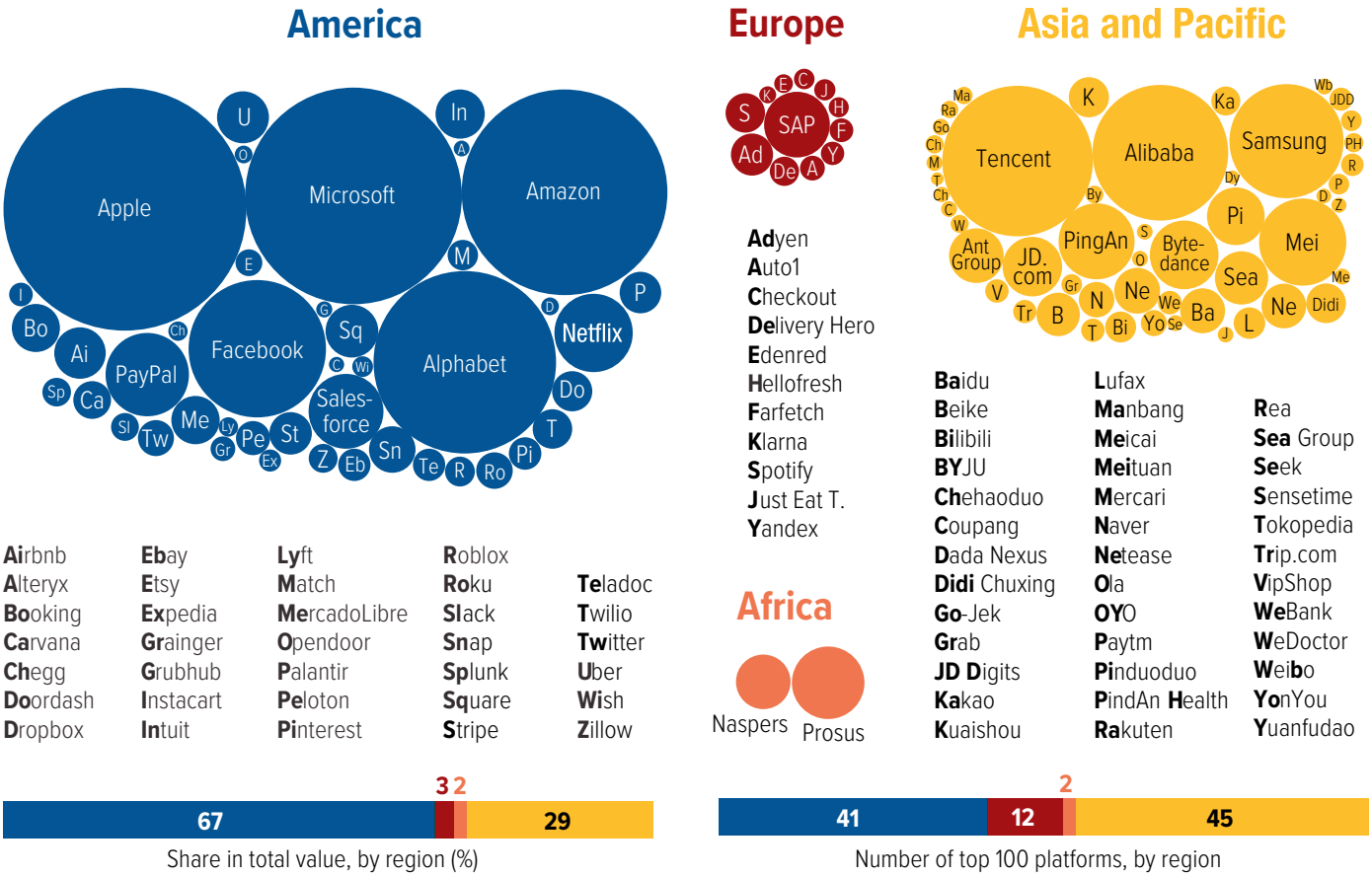
In the short term, this approach has made the EU a global leader in digital regulation. The GDPR, for example, now constitutes the de facto international standard for handling personal data, and is observed by major companies and adopted by other governments around the world. In the medium and longer term, however, this approach may be counterproductive. First, there is no indication so far that global regulatory leadership—including in areas beyond data privacy—will lead to the development and growth of globally significant EU companies, or to EU leadership in emerging technologies. It may happen, but other internal obstacles, such as a lack of adequate venture capital and divergences among member states' markets, are likely to continue frustrating European ambitions.

Second, the unilateralism of the European approach endangers the multilateral framework for global trade and, thus, also erodes transatlantic cooperation more broadly. World Trade Organization (WTO) rules applying to the digital economy are partial and dated, and efforts to update them through plurilateral trade negotiations have moved slowly. While every jurisdiction has the legal right to regulate as it sees fit, the current EU approach requires that other countries effectively adhere to EU rules, even in their own territory, or else they will be excluded from an exceptionally valuable market. If other jurisdictions were to act in the same way as the EU, the digital world would quickly divide into separate blocs with differing rules—and it is entirely possible that the United States and EU would be in different blocs.

Instead, the EU, United States, and other likeminded democratic governments should be working together to build a consensus that defends the true dividing line in the global digital economy. Only by working together can democracies collectively address the challenges posed by those countries that seek to use technology and digital rules to reinforce their own authoritarian approaches. Collaboration will require that both the EU and the United States examine their own policies and practices to ensure that companies are treated fairly and equally on both sides of the Atlantic, and that consumers enjoy sufficient protections. For the EU and its member states, this will mean reconsidering those emerging instances in which only EU companies may be allowed to provide certain services. Similarly, practices relating to government procurement should be addressed in Europe and the United States. The US-EU Trade and Technology Council (TTC) is becoming a useful forum for these discussions, but the United States, EU, and other likeminded governments should also examine multilateral institutions and their potential role in building consensus.

European Commissioner for the Internal Market Thierry Breton holds a news conference on a plan to boost the chip industry with the European Chips Act in Brussels, Belgium. February 8, 2022. REUTERS/Yves Herman.

Distribution of Top 100 Digital Platforms by Market Capitalization, 2021



Source: UNCTAD Digital Economy Report 2021. Holger Schmidt, available at www.netzoekonom.de/vortraege/#tab-id-1 (data as of May 2021). *Note:* As a reference, the market capitalization of Apple is $2.22 trillion, while for Mercado Libre it is $88.7 billion, $80.2 billion for Baidu and $59.7 billion for Spotify.

Europe's Digital Ambitions

When EU leaders began to focus on the digital economy, they quickly realized that Europe was at a competitive disadvantage. While the EU had strong national telecommunications companies and a few major software and hardware firms—SAP, Nokia, Spotify, Booking.com, Ericsson—there were no EU-based firms in the league of Amazon, Microsoft, Facebook (now Meta), Apple, or Google. Even as recently as 2021, EU-based platforms included only a dozen companies in the top global one hundred, and represented only 3 percent of its total value.[4] According to the European Commission's "Digital Compass" report, "digital technologies are mostly developed outside of the EU," with 90 percent of EU data managed by US companies, and EU-made microchips making up only 10 percent of the European market.[5]

However, the push for EU digital sovereignty was not based only on these technological and business shortcomings. It also drew on four other strands of thinking in the European policy arena.

First, the 2013 revelations by Edward Snowden about bulk electronic surveillance—including of Europeans—by the US National Security Agency (NSA) led to a harsh reaction in many countries, especially Germany. Snowden uncomfortably highlighted the difficulty in keeping the personal information of European citizens private and secure, while also creating suspicion and resentment against US agencies and companies, which persists in some quarters to this day. More recently, the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, which requires companies within US jurisdiction to provide federal law enforcement with access

4 Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2022* (Washington, DC: Foreign Policy Institute, Johns Hopkins SAIS/Transatlantic Leadership Network), 56.

5 "2030 Digital Compass," 3.

A woman shows her digital COVID-19 certificate at Naples Central Station, Italy. September 1, 2021. REUTERS/Ciro De Luca.

to foreign-located personal data, has reinforced those concerns. Indeed, in 2019, the European Data Protection Board—an EU-wide privacy-oversight institution—released an opinion stating that, due to the US CLOUD Act, service providers in the EU could find themselves "susceptible to facing a conflict of laws between US law and the GDPR and other applicable EU or national law of the Member States."[6]

Second, this perception of European weakness at the hands of the NSA and Department of Justice coincided with a growing debate in Europe over the need for "strategic autonomy" in the security and defense sphere. Over the past few years, in the wake of the instability and unpredictability of the Donald Trump administration, some EU leaders have emphasized the need for strong, homegrown EU military capabilities to overcome dependencies on the United States. In this view, Europe should push its defense industries to work across national borders and streamline their military research and development (R&D) and acquisitions, while also working closely with the United States in the NATO Alliance. The Russian invasion of Ukraine elevated NATO's importance in many EU member states—and even prompted Finland and Sweden to join the Alliance—but the EU itself possesses numerous regulatory and financial instruments for strengthening the EU defense-industrial base, including subsidies, procurement planning, and research support.

As the EU seeks strategic autonomy in terms of its defense resources, similar conversations about key sectors and technologies—including cyber defense, resilient information-technology (IT) infrastructure, and a strong digital industrial base—have also increasingly come to be framed as part and parcel of digital sovereignty. Commissioner Thierry Breton has described the United States and China as engaging in "technological war" and noted that, "In

6 Kristof van Quathem and Nicholas Shepherd, "European Data Protection Board Issues Opinion on US CLOUD Act," Covington, July 23, 2019, https://www.insideprivacy.com/data-privacy/european-data-protection-board-issues-opinion-on-u-s-cloud-act.

terms of security and defense, strengthening technological autonomy is now essential" for Europe.[7]

Third, the COVID-19 pandemic and the explosion of online education and work brought the importance of digital policy to the fore. It also demonstrated the perils of supply-chain vulnerabilities, including dependence on any other country for essential goods or services, including vital technologies or digital services. Previous European Commission President Jean-Claude Juncker had already encouraged the strengthening of the EU digital economy by attempting to remove barriers through the Digital Single Market initiative. Even before the pandemic, the current von der Leyen commission quickly identified "Europe fit for a digital age" as one of two major priorities. COVID-19 only strengthened the urgency of addressing digital issues, with 20 percent of the funds allocated under the COVID national-recovery plans to be dedicated to digital infrastructure and technologies.

Fourth, the EU has finally woken up to the dangers inherent in relying on companies and technologies from countries whose motives may be more geopolitical than commercial. The US campaign to persuade European governments to remove Huawei components from their fifth-generation (5G) infrastructure coincided with Europe's recognition of China as a "systemic rival" in March 2019.[8] In January 2020, the commission issued a "toolbox" aimed at enhancing security of 5G networks, which laid out criteria for trusted vendors, including that they have sufficient independence from their home governments. The Russian invasion of Ukraine has only exacerbated this sense of vulnerability, especially to cyberattacks, and also highlighted Europe's reliance on Russian supply of rare minerals used in batteries and other technologies. Coupled with the experience of COVID-19, the changing geopolitical situation thoroughly demonstrated the need for resilient online systems and infrastructure.

"Open Strategic Autonomy" in Trade

This search for autonomy also dovetailed with a recalibration in EU trade policy, away from a focus on seeking greater openness and toward reciprocity in trade relations. Following the imposition by the Trump administration of tariffs on steel and aluminum—and the US threat of tariffs in other disputes—the European Commission realized that it did not have the authority to respond to foreign coercive trade measures with its own countermeasures, but instead needed to rely on the now-stalled WTO dispute-settlement mechanism. As the Trump administration left office, China's trade embargo on Lithuania reinforced the commission's concerns. As the Director General of the Directorate-General (DG) for Trade Sabine Weyand commented, there had been a "shift in the international order from a rules-based system to a power-based system," and the EU "must accept this duality, whereby we continue to defend a multilateral order based on rules, but also accept that it is essential to do so from a stronger position, equipping ourselves with all necessary instruments."[9]

DG Trade coined the term "open strategic autonomy" to describe its new philosophy, and Weyand has been careful to balance references to autonomy with equivalent mention of openness: "If we define an actor's strategic autonomy as its ability to defend and pursue its interests, not alone but without undesirable dependence and without excessive constraints, it means that this strategy, in the economic field, is above all based on a principle of openness to the world."[10]

DG Trade still sees World Trade Organization instruments and reform as important in a world in which accelerating Chinese economic and geopolitical assertiveness can affect European interests. For example, in January 2022 the commission initiated a WTO dispute-settlement proceeding challenging China's interruption of bilateral trade with Lithuania, after Lithuania allowed Taiwan to establish representation in Vilnius.[11]

But the WTO is no longer seen as entirely sufficient to protect EU interests. In December 2021, the commission released its proposal for an "anti-coercion instrument" aimed at protecting the EU and its member states from economic coercion by third countries.[12] The proposal is currently undergoing legislative consideration by the Council of Ministers and the European Parliament. Once the legislation is adopted, potential EU countermeasures could include imposing customs duties on EU imports from third countries, placing restrictions on cross-border provision of services (including digital ones), or excluding a foreign

7 "Europe: The Keys to Sovereignty," European Commission, September 11, 2020, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.

8 "EU-China—A Strategic Outlook," European Commission and HR/VP Contribution to the European Council, March 12, 2019, 1, https://ec.europa.eu/info/publications/eu-china-strategic-outlook-commission-contribution-european-council-21-22-march-2019_en.

9 Sebastian Lumet, "The Double Integration Doctrine, a Conversation with Sabine Weyand," Groupe D'études Géopolitiques, January 31, 2022, https://geopolitique.eu/en/2022/01/31/the-double-integration-doctrine-sabine-weyand/.

10 Ibid.

11 Stuart Lau, "EU Sues China in WTO over Lithuania Blockade," *Politico*, January 27, 2022, https://www.politico.eu/article/eu-sues-china-wto-lithuania-blockade/.

12 "Proposal for a Regulation of the European Parliament and of the Council on the Protection of the Union and Its Member States from Economic Coercion by Third Countries," European Commission, December 8, 2021, https://trade.ec.europa.eu/doclib/docs/2021/december/tradoc_159958.pdf.

President of the European Council Charles Michel speaks with Director-General of the World Trade Organization Ngozi Okonjo-Iweala before a meeting in Brussels, Belgium. May 19, 2021. John Thys/Pool via REUTERS.

country from European public procurement. Weyand describes the proposed anti-coercion regulation as "a perfect example of the idea of open strategic autonomy because it gives us the ability to act according to our interests while preserving our openness."[13] More bluntly put, it would give the EU a flexible set of tools to combat hostile foreign conduct, such as punitive Chinese restrictions on trade with Lithuania or the Trump administration's (now-suspended) tariffs on European steel and aluminum.

Of course, Europe is not alone in seeking to reduce the vulnerabilities that international trade may present in an open market economy. The Joe Biden administration has been slow to remove Trump administration tariffs, and has reoriented US trade policy to be more mindful of the impact on labor. Nor is Europe isolated in its concerns about resilient infrastructure and supply chains. The United States and many other countries have also sought to reduce vulnerabilities in the wake of COVID-19 and growing geopolitical instability. Just as Europe has its policy initiative to support semiconductor manufacturing in the EU—the European Chips Act—so does the United States.[14] In short, the United States and European Union have taken parallel steps to reduce vulnerabilities to trading partners, and to international developments.

From Trade to Industrial Policy

EU leaders see the digital economy, along with the green economy, as essential for Europe's future prosperity. They want the EU to be at the forefront of innovation, as well as leading in writing rules that will protect the security and privacy of its citizens, networks, and infrastructure. In their view, EU citizens, networks, and infrastructure should not be entirely dependent on foreign companies, even those companies with long histories of engagement in Europe.

13 Lumet, "The Double Integration Doctrine, a Conversation with Sabine Weyand."

14 "CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China," White House, August 9, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

A statue of Lady Justice stands outside the EU Commission headquarters during a protest in Brussels, Belgium. April 29, 2019. REUTERS/Francois Lenoir.

To achieve these aims, the EU has taken a comprehensive approach, starting with supporting R&D but also aiming to facilitate innovation and manufacturing with projects like GAIA-X and the European Battery Alliance. It has sought to protect its citizens and businesses by vigorously enforcing rules on privacy and taking an aggressive stand on competition policy. For example, the EU requires that other countries implement data-protection rules equivalent to its own or face obstacles to—or even bans on—the transfer of personal data of EU residents. Now, with the Data Act, a similar regulatory regime may be adopted for non-personal data (often called "industrial data" in Europe). There is also a looming EU decision over the criteria for certifying cloud-service providers, and whether certification should be restricted to EU companies in some circumstances.

But many specifics of the operationalization of digital sovereignty remain unclear. Will the EU insist on moving forward on its own, regardless of the impact on close allies and likeminded partners? Will the United States and other partners—which face many of the same concerns about digital security and resilience—be able to work with the EU to ensure that democracies are united in their approach to the digital economy? Or will a divide arise across the Atlantic that authoritarian regimes can exploit as they seek to use the Internet for their own purposes? Much will depend on the EU's willingness to ensure that its market remains open, and that its rules do not discriminate or force unneeded localization.

Schrems and the Europeanization of International Data Transfers

Perhaps the most striking example to date of the press for digital sovereignty comes from the experience of implementing European data-protection law, as played out in the two *Schrems* decisions at the European Court of Justice (ECJ). Although the European Commission had decided in 2001 that transfers of EU personal data to the United States were adequately protected under the Safe Harbor arrangement, this decision was overturned by the ECJ in *Schrems I,* following the 2013 Snowden revelations. Since then, Washington and Brussels have struggled to maintain a functioning legal framework for the thriving business

of transatlantic transfers of personal data for commercial purposes.

In July 2020, the ECJ handed down its judgment in *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (colloquially known as *Schrems II*), agreeing with the eponymous Austrian privacy activist that the EU-US Privacy Shield Framework—successor to the Safe Harbor—failed to satisfy the requirements of EU fundamental-rights law.[15] The immediate result was that more than 5,300 companies—European as well as American, small as well as large—could no longer rely on that arrangement as a basis for transferring personal data from Europe to the United States.[16]

Overnight, companies were forced to find other methods for protecting privacy interests in transferred data. Most chose to rely on standard contractual clauses (SCCs), protective clauses preapproved by EU privacy authorities. But SCCs had also been deemed suspect by the *Schrems II* court, so the European Data Protection Board (EDPB) subsequently recommended bolstering them through supplementary measures, such as encryption and corporate commitments to resist US government data access.[17] However, the EDPB warned that, under certain circumstances, even these additional measures would be insufficient, leaving no lawful means of transatlantic data transfer.

The legality of relying on SCCs to transfer data has since been further eroded. Max Schrems' privacy-advocacy group, None of Your Business (NOYB), has brought more than one hundred challenges before privacy regulators to European companies' reliance on Google's and Facebook's data-analytics services, which entail transatlantic data transfers pursuant to standard clauses.[18] Two years on, data-protection authorities (DPAs) in several EU member states have begun to issue rulings in these cases. The authority in Schrems' home state, Austria, decided in April 2022 that an Austrian health website could not utilize Google Analytics to better understand who was using its services, because exporting data in the form of IP addresses to the United States opened the door for monitoring of individuals by "US intelligence services."[19] The French DPA (CNIL) insisted that the supplementary measures put in place by three French retailers that rely on Google Analytics were insufficient "because they do not exclude the possibility of access to personal data by US government agencies."[20]

Data activist Max Schrems speaks to the media on his allegations against Facebook in a courthouse in Vienna, Austria. April 9, 2015. REUTERS/Leonhard Foeger.

These rulings rest on the proposition that no theoretical risk of foreign-government access may be tolerated when personal data leave the EU for the United States—and, thus, conclude that the only safe course for European companies is to refrain from certain common types of data transfers to the United States. Similar rulings have emerged from Denmark, Germany, and Italy, among other EU countries.

As a prominent Dutch privacy lawyer and defender of the GDPR concedes, complying with *Schrems II* and EDPB supplementary measures is "mission impossible." She writes that, "Frustrations increase as companies work towards *Schrems II* compliance by executing mitigating measures… [yet] DPAs increasingly adopt an absolutist approach,

15 Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, C-311/18, July 16, 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=230683&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=344153.

16 Kenneth Propp and Peter Swire, "Geopolitical Implications of the European Court's Schrems II Decision," Lawfare, July 17, 2020, https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.

17 "Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data," European Data Protection Board, June 18, 2021, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

18 "EU-US Transfers Complaint Overview," noyb, last visited September 12, 2022, https://noyb.eu/en/eu-us-transfers-complaint-overview.

19 Data protection complaint (Art. 77 (1) DSGVO), Austrian Data Protection Authority, April 22, 2022, https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf.

20 "Use of Google Analytics and Data Transfers to the United States: the CNIL Orders a Website Manager/Operator to Comply," Commission Nationale de l'Informatique et des Libertés, February 10, 2022, https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply.

US President Joe Biden and European Commission President Ursula von der Leyen shake hands after holding a joint press conference, where they announced a political agreement on a new US-EU data privacy framework, in Brussels, Belgium. March 25, 2022. REUTERS/Evelyn Hockstein.

whereby mitigating measures are disregarded irrespective of the actual risk for data protection after transfer."[21]

The US government has vainly tried, by means short of legislation, to persuade European privacy authorities that it does not exploit EU-origin personal data transferred for commercial purposes. A 2020 white paper, collectively issued by the Departments of Commerce and Justice and the Office of the Director of National Intelligence, insisted, "Companies whose EU operations involve ordinary commercial products or services, and whose EU-US transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe US intelligence agencies would seek to collect that data."[22] In response to the Austrian DPA ruling, Google's general counsel publicly directed a similar message to European privacy authorities: "Google has offered Analytics-related services to global businesses for more than 15 years and in all that time has never once received the type of demand the DPA speculated about. And we don't expect to receive one because such a demand would be unlikely to fall within the narrow scope of the relevant law."[23] While European privacy officials maintain that these special safeguards are required to make international data transfers consistent with EU fundamental rights law, a leading Washington think-tank

21 Lokke Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers: It's the Geopolitics, Stupid!*" Future of Privacy Forum, April 4, 2022, https://fpf.org/blog/the-eb-and-flow-of-trans-atlantic-data-transfers-its-the-geopolitics-stupid/.

22 "Information on US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after Schrems II," US Department of Commerce, US Department of Justice, and Office of the Director of National Intelligence, September 2020, 2, https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

23 Kent Walker, "It's Time for a New EU-US Data Transfer Framework," *Google in Europe blog*, January 19, 2022, https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/.

observer suspects that "allegations of surveillance by US intelligence agencies have become a justifying narrative for tech governance, data localization, and the European quest for tech sovereignty."[24]

In March 2022, European Commission President von der Leyen and President Biden announced a new agreement in principle on transatlantic data transfers to improve deficient features of Privacy Shield.[25] The Trans-Atlantic Data Privacy Framework contains a US intelligence-agency commitment to limit access to data to what is "necessary and proportionate" to protect national security—the same standard required under European fundamental rights law. The US government also promises to adopt new procedures to ensure more effective oversight of its foreign intelligence activities, and to empower a new administrative redress tribunal to investigate and resolve Europeans' allegations that their personal data have been unlawfully accessed. The United States will apply these new protections not only to transfers made under this new arrangement, but also to those relying on SCCs.

It is too soon to say whether the new transatlantic data-transfer framework will definitively resolve the tension between EU privacy law and the international transfer of personal data. The agreement in principle must be translated into binding changes in US law via an executive order and a Justice Department regulation, and then be reflected in a European Commission adequacy finding—processes that could easily take until the end of 2022, or beyond. Max Schrems has already signaled his skepticism of the new deal, labeling it "lipstick on a pig," and all but promising to challenge it again at the ECJ.[26] Doubtless there are elements of the new arrangement that will be closely questioned by the court. Even if the new arrangement persists, the experience of the last ten years has demonstrated the extraterritorial impact of EU data protection law and the difficulties of reconciling it with the international free flow of personal data.

24 James Andrew Lewis, "Surveillance Fears and Privacy Shield," Center for Strategic and International Studies, April 4, 2022, https://www.csis.org/analysis/surveillance-fears-and-privacy-shield.

25 "United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework," White House, March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/.

26 Schrems quoted in Vincent Manancourt and Mark Scott "The West's Plan to Keep Global Data Flows Alive," *Politico*, March 31, 2022, https://www.politico.eu/article/data-oecd-privacy-shield-national-security/. "'Privacy Shield 2.0?': First Reaction by Max Schrems," noyb, March 25, 2022, https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems.

Digital Sovereignty and the von der Leyen Commission

While the EU's efforts to protect the personal data of its citizens go back many years, the von der Leyen commission—encouraged by the European Parliament—has significantly expanded the scope of EU digital policy. In doing so, the European Commission and Parliament have put achieving digital sovereignty at the forefront of their agendas.

The most comprehensive statement of this ambition is the commission's "Digital Compass," which declares that the EU needs to address its strategic weaknesses, vulnerabilities, and high-risk dependencies in the digital sphere: "That is the way for Europe to be digitally sovereign in an interconnected world by building and deploying technological capabilities in a way that empowers people and businesses to seize the potential of the digital transformation."[27] The compass also predicts that the EU's digital partnerships with other countries "will promote alignment or convergence with EU regulatory norms and standards on issues such as data protection, privacy and data flows, the ethical use of AI, cybersecurity and trust, tackling disinformation and illegal content online, ensuring internet governance, and supporting development of digital finance and e-government."[28]

President von der Leyen has made building "A Europe fit for a Digital Age" one of two key priorities for her commission (along with the Green Deal). Only a few months after taking office, the commission moved beyond rhetoric to outline its plans for a comprehensive legislative agenda, including measures to:

- increase digital access and skills across Europe;
- protect employees working in the digital economy;
- boost EU funding for key technologies;
- enhance the security and resilience of networks and infrastructure;
- establish restrictions on market-dominating companies;
- set rules for the use of new technologies, including AI;
- ensure the removal of illegal content and goods from online platforms; and
- establish a European market for non-personal data.[29]

The commission has proposed several major legislative packages on these subjects, which are making their way through the EU process.

In 2020, the commission introduced proposals for three key pieces of legislation, which made clear the direction of the EU's digital agenda, and also demonstrated the tensions between an open digital economy and the EU's sovereign ambitions. All these proposals would impose requirements on non-EU companies operating in the European market, as is normal with any domestic regulatory system. In addition, some of these proposals included elements that could be regarded as discriminatory; in some

European Commission President Ursula von der Leyen delivers the State of the European Union address in Strasbourg, France. "A Europe fit for the digital age" is one of the von der Leyen Commission priorities. September 15, 2021. REUTERS/Yves Herman/Pool.

27 "2030 Digital Compass," 1.

28 Ibid., 19.

29 "Shaping Europe's Digital Future," European Commission, February 2020, https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

cases, these were scaled back as consideration of the proposal advanced. In all cases, the European Commission and European Parliament clearly regarded the legislation as a model for global rules. These legislative packages included the following.

- **The Digital Services Act (DSA)**, which imposes numerous obligations on platforms operating in the EU, including requirements related to identifying and removing illegal content, and combating illegal and counterfeit goods and illegal hate speech. Companies expressed numerous concerns, ranging from protecting algorithms and other intellectual property to elaborating conditions of content removal. The DSA applies equally to EU-based platforms and non-EU platforms offering their services in the EU. It received final approval in July 2022.

- **The Digital Markets Act (DMA)**, which imposes significant constraints on the competitive behavior of the largest platforms, designated as "gatekeepers" to the digital economy. Gatekeepers would be prohibited from preferencing their own products and services, and from using data across different services. Initially, this proposal appeared to be aimed exclusively at the major US platforms (i.e., GAFA—or Google, Amazon, Facebook, and Apple—and sometimes including Microsoft), a conclusion reinforced by the statements of some key EU leaders.[30] After negotiations between the European Parliament and the Council of Ministers widened the definition of gatekeeper, it is now expected that the initial list may include both EU and Chinese companies, as well as the US platforms. Assuming that the gatekeepers to be identified by the commission include a number of non-US companies, and that implementation does not introduce any potential discriminatory elements, it would be fair to conclude that the EU is unwilling to risk the nationality-based discrimination that a US-only list of gatekeepers would require. The DMA also received final approval in July 2022, with the list of gatekeepers to be identified by spring 2023.

- **The Artificial Intelligence Act** establishes rules for the use of AI throughout the EU, aimed at creating a standard for "trustworthy" and "human-centric" AI. It distinguishes between high-risk and limited-risk AI, with most applications falling in the latter category. A few exceptionally egregious uses of AI are expected to be banned, including real-time facial recognition used for surveillance. The AI Act would apply to the importation into the EU of goods or services that incorporate the technology; those imports will be required to go

Source: "Shaping Europe's Digital Future," compiled by the Atlantic Council.

30 See, for example, Andreas Schwab's comments in Javier Espinoza, "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.

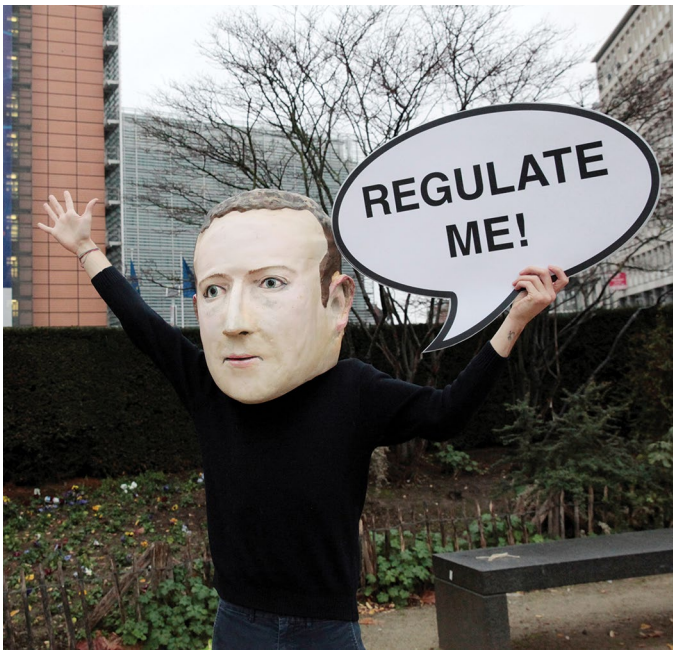
through a conformity-assessment process to ensure that they meet EU standards. The proposed AI Act is still relatively early in the legislative process, with the Parliament and the Council not yet agreed on their final positions. Yet it is already clear the EU intends this as a landmark piece of legislation that will push other jurisdictions to adopt EU standards for trustworthy AI in their own domestic regulatory regimes.

Although these initial pieces of legislation generated much angst among opponents of the EU's traditional regulation-heavy approach, they ended up not being explicitly discriminatory (assuming the DMA gatekeepers are identified as expected). They are clearly intended as models for other jurisdictions, and certainly other rule-makers, including some members of the US Congress, are looking to the DSA and DMA for inspiration. But other pending EU regulatory moves in a few key areas—non-personal data, cybersecurity, and cloud—could well discriminate against non-EU companies or limit their ability to transfer data abroad. These additional proposals are not yet finalized, and potentially discriminatory elements could be removed. But for the moment, these proposals highlight the sometimes-exclusionary nature of the EU's search for digital sovereignty.

Industrial Data: The Next Frontier for Digital Sovereignty

With GDPR already established as the de facto global standard for protecting personal data transferred outside the EU, the von der Leyen commission has shifted its attention to fashioning comparable protections for international transfers of non-personal data. A recent economic study found that commercially sensitive non-personal data are the most common type of data to be shared across borders.[31]

The commission's 2020 Data Strategy envisioned two separate measures addressing non-personal data—the Data Governance Act (DGA) and the Data Act (DA).[32] The former was approved by EU legislators in late 2021, while the commission proposed the latter, now undergoing Council of Ministers and Parliament consideration, in February 2022.



A protester wears a mask of Facebook CEO Mark Zuckerberg during a protest in Brussels, Belgium. December 15, 2020. REUTERS/Francois Walschaerts.

The Data Governance Act aims to facilitate the 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. Many of these public-sector-held datasets contain non-personal information, and their potential reuse is complicated by protections for privacy, intellectual property or trade secrets, or other business confidentiality protections. Commissioner Breton was characteristically geopolitical when announcing the proposed DGA: the commission's goal was "an open yet sovereign European Single Market for data."[33] Vice President Vestager expressed a similar sentiment: the Data Governance Act offered "an alternative model to the current data-handling practices offered by Big Tech platforms."[34]

In the wake of the COVID-19 pandemic, the commission also has proposed a sector-specific European Health Data Space regulation.[35] It would incorporate the Data

31 Sarah Snelson and Federico Cilauro, "Beyond Personal Data: The Cost of Data Flow Restrictions to EU Companies," Frontier Economics, February 17, 2022, https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf.

32 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data," European Commission, February 19, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066; "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)," Council of the European Union, December 10, 2021, https://data.consilium.europa.eu/doc/document/ST-14606-2021-INIT/en/pdf; "Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy," European Commission, February 23, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

33 Thierry Breton quoted in "Commission Proposes Measures to Boost Data Sharing and Support European Data Spaces," European Commission, November 25, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2102.

34 Ibid.

35 "Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space," European Commission, May 5, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197&from=EN.

Governance Act and Data Act frameworks for secondary use of data. Sector-specific regulations for other types of non-personal data—due to number nine in all—are under development as well.

The Data Act, which is now going through the legislative process, concentrates on expanding business-to-business (B2B) sharing of non-personal data. EU leaders anticipate that the DGA and DA, by establishing rules for the secondary use, transfer, and monetization of industrial data, will create a valuable and innovative commercial opportunity for European companies rivaling the data exploitation currently conducted primarily within large and mostly US companies.

However, reuse of privately held industrial data is often complicated by the same intellectual property and trade secret rules as is the case for government-held data. Moreover, cloud-service users often choose to store EU-origin non-personal data on servers located in third countries. According to the commission, EU companies "report reluctance to use cloud services due to concerns of unlawful or unauthorized access that may lead to IP theft [or] industrial espionage." This reflects a "trust problem," and "the trustworthiness of cloud services equals the trustworthiness of the data economy," according to the impact assessment for the Data Act.[36]

Both the DGA and Data Act attempt to resolve this trust problem by erecting complex safeguards that would complicate data transfer outside the European Union. The commission justifies incorporating such restrictions into otherwise liberalizing measures by citing a threat also invoked in the GDPR—extraterritorial governmental access laws. The impact assessment identifies two US signals intelligence authorities, Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, as well as China's 2017 National Intelligence Law.[37] The commission also cites the US CLOUD Act, which allows US law enforcement to demand information held abroad by communications service providers subject to US jurisdiction.[38]

The US government has consistently denied deploying its foreign intelligence surveillance apparatus to benefit US companies. "US government commitments and public policy…expressly prohibit the collection of information for the purpose of obtaining a commercial advantage," a 2020 white paper asserts.[39] Nonetheless, the Data Governance Act and the Data Act proceed on the premise that the United States, along with China, does so. The widespread belief in Europe that US law enforcement agencies would use the CLOUD Act, a unilateral criminal evidence-gathering power, for US corporate commercial advantage is also unproven.

Nevertheless, to combat this threat, the DGA (Article 30) and proposed Data Act (Article 27) require data holders entering into foreign transfers to "take all reasonable technical, legal and organizational measures, including contractual arrangements" to avoid falling prey to foreign-governmental access law. The reference to "technical, legal and organizational" safeguards draws on the recommendations developed for personal data transfers by the European Data Protection Board, in the wake of the Court of Justice's *Schrems II* judgment.[40]

In addition to taking these safeguard measures, a data holder under the DGA or DA may honor only those unilateral foreign access requests that it deems to be reasoned, proportionate, and specific. Requests must also be subject to review by a third-country court or tribunal that would balance the competing domestic and foreign interests. The required analysis must be conducted on a case-by-case basis, as no country-specific "adequacy" findings are envisioned.

Under these rules, e-data holders would face a novel and difficult task in ensuring that international transfers of non-personal data protected by intellectual-property laws are safeguarded from potential third country surveillance. The challenge will be compounded by the potential interaction of the DGA and DA with the GDPR data-transfer regime, as two scholars have noted.[41]

In these circumstances, the easiest course of action for most data holders will be to avoid third-country transfers of non-personal data. A recent survey reported that, since the invalidation of the Privacy Shield Framework, transfers of personal data from the EU to the United States have

36 "Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)," European Commission, February 23, 2022, 20, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

37 "Executive Order 12333—United States Intelligence Activities," Office of the Federal Register, December 4, 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html; Foreign Intelligence Surveillance, 50 US Code Chapter 36, Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/50/chapter-36.

38 Clarifying Lawful Overseas Use of Data (CLOUD) Act, PL 115-141, Division V (2018), https://www.justice.gov/dag/page/file/1152896/download.

39 "Information on US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after Schrems II," 2.

40 "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)," 57.

41 Inge Graef and Martin Husovec, "Seven Things to Improve in the Data Act," Social Science Research Network, March 7, 2022, https://ssrn.com/abstract=4051793.

EU Digital Initiatives

INITIATIVE	PURPOSE	STATUS
General Data Protection Regulation	Governs the collection, processing, and transfer of personal data located in EU territories	**Regulation entered into force May 2018**
Directive on Copyright in the Digital Single Market	Requires online platforms to provide remuneration for creators and publishers when their content is used online	**Directive entered into force June 2019**
EU Cybersecurity Act	Establishes a cybersecurity certification framework and expands remit of the EU's cyber agency, ENISA	**Regulation entered into force June 2019**
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**
Data Governance Act	Facilitates the sharing of public sector, non-personal data to enhance innovation in the EU	**Regulation entered into force June 2022**
European Democracy Action Plan	Outlines anticipated proposal for legislation governing political ads and other rules intended to safeguard democratic processes, including elections	**Published December 2020**
Digital Services Act (DSA)	Retains intermediate liability protections for online platforms but also established common rules for platforms' content moderation and reporting requirements	**Regulation published in the Official Journal October 2022**
Digital Markets Act (DMA)	Establishes specialized competition rules for large digital platforms identified as "gatekeepers"	**Regulation published in the Official Journal October 2022**
Artificial Intelligence Act	Aims to regulate the development and use of AI, especially "high-risk" AI, to ensure a human-centric and trustworthy technology	**Regulation proposed April 2021**
Common Chargers Rule in Radio Equipment Directive	Establishes common charging ports for manufacturers of portable electronic devices to improve consumer welfare and reduce waste	**Directive provisionally agreed June 2022**
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	**Directive provisionally agreed May 2022**
Data Act	Aimed at stimulating EU innovation and competitiveness through the development of a market for non-personal, industrial data	**Regulation proposed February 2022**
European Chips Act	Would develop the EU's semiconductor capacity with government subsidies and public and private investments	**Regulation proposed February 2022**
Cyber Resilience Act	Would establish cybersecurity rules on connected products and services for manufacturers and vendors	**Regulation proposed September 2022**
Product Liability Directive Revision	Would update liability rules on product risks associated with digital and green transitions	**Proposed September 2022**
Artificial Intelligence Liability Directive	Would establish uniform rules for civil liability of damages caused by AI systems	**Proposed September 2022**

Source: European Commission compiled by the Atlantic Council.

declined by about one-quarter. Technology industry groups predict that adding mandatory legal safeguards for international flows of non-personal data similarly would lead EU companies—as many as 40 percent of them, according to the previously noted economic study—to respond by localizing data within EU territory.[42] In its push for "data sovereignty," the EU risks blocking the international flow of industrial data—even to allies and likeminded partners—unless they can meet practically unattainable standards of protection on a case-by-case basis.

Data Sovereignty: Lost in the Cloud?

EU leaders have long recognized cloud services as a key part of digital infrastructure, and have highlighted the importance of home-grown cloud services as an element in achieving digital sovereignty. In 2019, the governments of France and Germany, in conjunction with a number of their major industrial companies, launched GAIA-X, an ambitious project to make cloud services interoperable and, thus, encourage the growth of smaller EU-based cloud providers.[43]

The GAIA-X initiative did not aim to create a single European cloud provider capable of competing with the three major US-based "hyperscalers"—Amazon Web Services (AWS), Microsoft, and Google—which collectively provide 70 percent of Europe's booming cloud-services market. Rather, the goal was to develop common technical standards and legal frameworks so that customers could move data around freely within the envisioned network, including to potential new EU-based services. "The GAIA-X project is not a comprehensive European policy," a leading European technology lawyer has written, "but it is a concrete realization of the open interfaces, standards, and interconnection needed for the European policy and is explicitly based on principles of *sovereignty-by-design*."[44]

Since the launch of GAIA-X, membership has grown to more than three hundred companies and organizations, including trade associations and research organizations as well as technology companies themselves. Major non-European cloud providers—including AWS, Microsoft, Huawei, and Alibaba—have joined, although only companies headquartered in Europe may serve on the GAIA-X governing board. The Chinese companies even sponsored GAIA-X's 2021 summit meeting, a move that prompted criticism from GAIA-X's former founding director. Some original European members have likewise complained about the strong participation of foreign companies in GAIA-X technical working groups. French cloud provider Scaleway withdrew from the project, with its chief executive officer (CEO), Yann Lechelle, publicly regretting "the fact that the association is largely influenced and financed by major US, and now Chinese businesses…right down to the technical working groups. While we defended a strictly European governance, the [foreign] influence is largely indirect and tactical, bypassing the initial nature of the governing body and by-law."[45]

As its governance structure has become more elaborate and its politics more fraught, GAIA-X has suffered repeated delays in developing the policy guidance and technical standards needed to become a commercial reality. Last October, French President Emmanuel Macron said that Europe was "very late" in developing its plans for promoting a European cloud, echoing a lament from his then digital Minister Cédric O that efforts needed to "go faster" because GAIA-X held "in their hands…no less than a part of France's digital sovereignty."[46]

Finally, in April 2022, GAIA-X released long-awaited policy objectives and labeling criteria that will form the main requirements of its emerging "trust" framework. The labeling criteria distinguish among three levels of service, with Level 3 targeting "the highest level of compliance" for "standards and expectations for data protection, security, transparency, portability, flexibility, and European control, fully aligning with EU regulations."[47] Specifically, Level 3 requires, among other things, that all data processing and storage be done within the EU. In addition, the provider must put safeguards in place to ensure that any foreign-government access requests comply with EU law—a requirement that expressly mirrors steps required under the GDPR, and potentially the Data Act, to resist extraterritorial legal process under the US CLOUD Act, for example. Level 3 providers must also have their main establishment in the European Union and no controlling

42 "IAPP-EY Annual Privacy Governance Report 2021," Ernst & Young and International Association of Privacy Professionals, 2021, https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf.

43 Burwell and Propp, *The European Union and the Search for Digital Sovereignty*, 9.

44 Moerel, "The Ebb and Flow of Trans-Atlantic Data Transfers."

45 Dominique Filippone, "Gaia-X : le Sponsoring Sino-Américain Agace, Scaleway S'en Va," *Le Monde Informatique*, November 18, 2021, https://www.lemondeinformatique.fr/actualites/lire-gaia-x-le-sponsoring-sino-americain-agace-scaleway-s-en-va-84841.html.

46 Pascal Samama, "Cloud Souverain: Emmanuel Macron Admet des 'Retards' Mais Poursuit les Investissements," *BFM Business*, October 12, 2021, https://www.bfmtv.com/economie/entreprises/industries/cloud-souverain-emmanuel-macron-admet-des-retards-mais-poursuit-les-investissements_AN-202110120257.html; Cédric O quoted in Clothilde Goujard and Laurens Cerulus, "Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project," *Politico*, October 26, 2021, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.

47 "Gaia-X Association Announces Labelling Framework Release," Gaia-X, December 9, 2021, https://gaia-x.eu/news/latest-news/gaia-x-association-announces-labelling-framework-release/.

The logo of French cloud computing company OVHcloud on a data center in Strasbourg, France. October 13, 2021. REUTERS/ Christian Hartmann.

foreign shareholders. Thus, it appears that a foreign provider would be able to participate in Level 3 activities only in cooperation with a controlling European partner. Non-European companies must demonstrate "their independence from non-European legislation or access from non-European actors," GAIA-X has announced, adding that "non-European players will be free to adapt to our sovereignty framework to operate in Europe."[48]

Meanwhile, European cloud service providers have also turned to EU antitrust law in an effort to blunt the dominance of US cloud services. Although Margrethe Vestager, the commission executive vice president overseeing competition policy, has stated that she sees no abuse of dominance by the market leaders to date, the Directorate General for Competition (DG COMP) has taken preliminary steps to respond to a complaint by German and French competitors NextCloud and OVHcloud. The commission has sent a questionnaire to companies stating that it "has information that Microsoft may be using its potentially dominant position in certain software markets to foreclose competition regarding certain cloud computing services."[49] Depending on the responses to the questionnaire, DG COMP could open a formal investigation.

Some major foreign cloud providers, faced with these headwinds, have begun to fashion their own alliances with European counterparts in order to satisfy the political appetite for localized services. Google has entered into arrangements with two French companies, Orange and Thales, and with T-Systems, a Deutsche Telekom affiliate in Germany.[50] Google's German venture, for example, would assign to its local partner such tasks as encryption and identity management, as well as granting T-Systems a voice in deciding how to respond to foreign data access requests.[51] Microsoft has also fashioned its own French offering with Orange and Capgemini, as well as offering an encrypted "cloud privacy service" for its German public cloud customers. A previous Microsoft partnership in Germany with T-Systems, launched in 2015, quietly folded in 2018 amid customer resistance to its cost and difficulty of use. Companies headquartered in the EU are not necessarily exempt from US law, however, if they do business in the United States or have other jurisdictional contacts there.[52]

The fate of GAIA-X has yet to be determined. Some observers have already written it off as yet another failing European industrial-policy foray into dynamic technology markets, while others see its slow emergence as only growing pains that may yet yield a significant competitive force. Certain US cloud providers appear to have acknowledged that Europe's ambitions for a sovereign cloud are not fleeting and, thus, have structured transatlantic joint ventures so that they can be insulated from foreign influence to a significant extent. This high-stakes contest will only continue as Europe seeks to create a sovereign cloud.

European Cybersecurity Regulation Takes a Sovereign Turn

In parallel with its efforts to safeguard its "sovereign" interest in protecting personal and non-personal data from

48 "Gaia-X Releases Its Latest Policy Rules and Labelling Criteria, Demonstrating Better Governance and Compliance with Gaia-X's Principles," Gaia-X, April 25, 2022, https://gaia-x.eu/news/latest-news/gaia-x-releases-its-latest-policy-rules-and-labelling-criteria-demonstrating-better-governance-and-compliance-with-gaia-xs-principles.

49 Paresh Dave, "Microsoft's Cloud Business Targeted by EU Antitrust Regulators," Reuters, April 1, 2022, https://www.reuters.com/business/microsofts-cloud-business-targeted-by-eu-antitrust-regulators-2022-04-01/.

50 Mathieu Rosemain, "France's Thales Creates Cloud Services Company Powered by Google," Reuters, June 30, 2022, https://www.reuters.com/technology/frances-thales-creates-cloud-services-company-powered-by-google-2022-06-30/.

51 David Meyer, "Germany's 'Sovereign Cloud' Is Coming—and It's Provided by Google," *Fortune*, September 8, 2021, https://fortune.com/2021/09/08/germany-sovereign-cloud-google-t-systems/.

52 Kenneth Propp, "European Cybersecurity Regulation Takes a Sovereign Turn," *European Law Blog,* September 12, 2022, https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

French officials Cédric O, then-Minister of State for Digital and Telecommunications, Bruno Le Maire, Minister of Economy Finance, and Clément Beaune, then- European Affairs Minister meet at the EU ministerial conference "Building Europe's Digital Sovereignty" during the French EU presidency in Paris, France. February 7, 2022. REUTERS/Sarah Meyssonnier.

foreign-government access—and to protect the cloud where data are largely stored—the EU has increasingly turned its attention to strengthening information security. Even though Europe's cybersecurity initiatives have been low profile, they—like its better-known privacy measures—have the potential to limit the services that foreign cloud providers and others may offer on the continent, to preclude them from competing for public procurement and critical-infrastructure contracts in Europe, and to force them to localize their operations. This effort is likely to grow in scope and speed.

France's cybersecurity agency, known as ANSSI, has led the way through its security certification and labeling program, SecNumCloud. Since launching SecNumCloud in 2016 as a voluntary scheme, France has certified as "trusted" only five services provided by three companies, all of which are headquartered in France.[53] Now the French government has acted to make certification requirements mandatory for cloud firms that wish to provide services to French government agencies or to private operators of essential services. In addition, cloud-service providers must commit to store and process data within the European Union, and to administer and supervise the services within the EU.

The goal, according to France's Trusted Cloud Doctrine policy statement, is that any qualifying cloud-service provider be "immune to any extra-EU regulation."[54] The revised SecNumCloud requirements, which took effect in March 2022, effectively force foreign-headquartered

53 "Liste des Produits et Services Qualifies," National Cybersecurity Agency of France (ANSSI), April 2, 2022, https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.

54 "Doctrine 'Cloud au Centre' Sur l'Usage de l'Informatique en Nuage au Sein de l'État," Ministry of Transformation and Public Service of the French Republic, July 5, 2021, https://www.transformation.gouv.fr/files/presse/Circulaire-n6282-SG-5072021-doctrineuutilisation-informatique-en-nuage-Etat.pdf.

cloud companies to enter into joint ventures with French providers in which the foreign participant owns a minority non-controlling interest, or else to license their technologies to a certified local vendor.[55]

The director general of ANSSI, Guillaume Poupard, was explicit about the motive. Europe needs "a rule that only European law is applicable on cloud products certified in Europe," he said, referencing a desire to "exclude the standard American and Chinese services" from offering services in critical sectors.[56] "This is about…having the courage to say that we don't want non-European law to apply to these services," Poupard added. "If we're not capable to say this, the notion of European sovereignty doesn't make sense."[57]

During its presidency of the EU in the first half of 2022, France pressed to extend its approach to the EU level, via the EU Cybersecurity Certification Scheme for Cloud Services (EUCS). The EU's Cybersecurity Act, adopted in 2019, established an EU-wide certification framework for information and communication technology (ICT) products and services. This is to be elaborated by the EU Agency for Cybersecurity (ENISA).[58] In December 2020, ENISA began a public consultation as the first step toward a new certification scheme.[59] A technical working group is preparing a proposal, expected to be presented to member-state experts and to the European Commission thereafter. A leaked version surfaced in June. The new requirements could be finalized by the end of the year.

The European Commission, in a working document, identified cloud services as a "strategic dependency," and expressed concerns that the EU cloud market is led by a few large cloud providers headquartered outside the EU.[60] France submitted a non-paper to the ENISA-led working group proposing that companies seeking to qualify as eligible to offer high-level services should meet four new criteria, including immunity from foreign law and localization of cloud-service operations and data within the EU. Although the EU-level cyber-certification requirements are currently conceived as voluntary for the most part, they could become effectively mandatory as the result of a just-completed revision of a separate law, the EU's Directive on Security of Network and Information Systems (NIS). Under the NIS2 Directive, which is likely to come into effect in 2023, many businesses across the EU will need to demonstrate compliance with cybersecurity measures and, thus, may look to adopt certification requirements for their IT components.

A cross-party group from the European Parliament, with heavy French representation, has weighed in to support the French proposal at ENISA. Member states' reactions, on the other hand, have been mixed. Seven of them—Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden—have submitted a non-paper to the Council of the European Union, questioning the need for sovereignty requirements in the new cyber-certification standards and calling for further study of their potential interaction with the GDPR, non-personal-data regulations, and EU international trade obligations.[61] In addition, these governments, along with Germany, have called for a political-level discussion of the subject in the Council of the European Union before the European Commission proceeds to finalize the new standards.

55 "Prestataires de Services d'Informatique en Nuage (SecNumCloud) Référentiel d'Exigences," National Information Systems Security Agency of the French Republic, 2021, https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a.pdf.

56 Laurens Cerulus, "France wants cyber rule to curb US access to EU data," *Politico*, September 13, 2021, https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.

57 Ibid.

58 Regulation of the European Parliament and of the Council ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), (EU) 2019/881, L151/15-69, April 17, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

59 "Cloud Certification Scheme: Building Trusted Cloud Services Across Europe," European Union Agency for Cybersecurity (ENISA), December 22, 2020, https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme/.

60 "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.

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

The Future of Digital Sovereignty?

Two and a half years after the von der Leyen commission launched its digital initiatives, there is now a clearer vision of EU digital sovereignty and how it is being realized.

- To support the development of European innovations and industries in key technologies, **the EU plans to dedicate large amounts of funding through Horizon Europe and other R&D initiatives,** as well as 20 percent of each national COVID-recovery and resilience-fund allocation.[62] Special programs such as GAIA-X, the Battery Alliance, and the EU Chips Act will bring even more funding to the task of developing cutting-edge technologies in the EU. In the past, such targeted industrial policies and potential subsidies would have raised concerns among some EU member states and foreign trading partners, but COVID and recent geopolitical concerns have meant that more countries are heading down this path in key sectors of their economies with fewer obstacles.

- **New EU measures on AI, data, competition, online content moderation, and other elements of the digital economy are aimed at becoming global standards, along the lines of the GDPR.** This strategy is expected to boost the influence of the EU by making it among the leading rule writers in the global digital economy. The market power of its four hundred and fifty million citizens, it is hoped, will ensure that major companies adopt EU rules at least for their European operations, if not globally. But as other bodies develop their own rules and standards, such as the Group of Seven (G7) initiative on Data Free Flow with Trust, or the Global Cross-Border Privacy Rules devised by Asia-Pacific Economic Cooperation (APEC) and now broadened in geographic scope, there is an increasing chance that the EU rules will clash with others, even those emanating from likeminded and allied countries.[63] As a consequence, key commercial activities, such as international data transfers and the export and import of goods and services incorporating AI, stand to become much more difficult, even among friends.

- In key areas, **new EU regulations will reinforce—or even require—localization in data management, ownership, and other key functions.** In some cases, this is based on an understandable desire to protect EU citizens and businesses from untrustworthy vendors. But by equating trust with immunity from non-EU laws, those rules can exclude not only Chinese firms, but also US, Japanese, Canadian, and even EU firms that are active in non-EU markets. While identifying trustworthy companies is an important task, this model of sovereignty may well lead the EU to digital autarky, forcing it to rely only on homegrown companies and technologies.

Why does it matter if the EU pursues this particular path toward digital sovereignty? The EU certainly has the right to regulate its domestic economy—including its digital economy. But at a time when Western democracies and their market economies are increasingly under threat, those who seek to tackle the excesses of the digital economy from a democratic and rules-based perspective should be acting together, not establishing rules that make cooperation more difficult.

The EU is central to the efforts of democracies to establish guardrails for the digital economy. Its huge market makes it attractive to companies from around the world; indeed, for US companies in 2019, Europe was the destination for more than 70 percent of the total information services supplied by their foreign affiliates. Europe is also key to the physical hubs and networks that make the Internet global. Hubs in Frankfurt, Amsterdam, Paris, and Stockholm (as well as London) provide more capacity than those in the United States or China.

But being a core partner in the global digital economy is also vital for Europe. In 2020, more than half (52 percent) of the EU27's 987 billion euros in digitally enabled services exports went to countries outside the EU, while 58 percent of its 986 billion euros in digitally enabled services imports came from non-EU countries.[64] Clearly, it would be to the economic disadvantage of the EU and of its current economic and investment partners—including the United

62 Horizon Europe has allocated 15 billion euros for "digital, industry, and space" projects during 2021–2027; the Digital Europe Program has 7.5 billion euros in funds during the same period, and the Next Generation EU COVID-recovery plan allocates 20 percent of its 750-billion-euro budget (i.e., 150 billion euros) to digital transformation.

63 "G7 Action Plan for Promoting Data Free Flow with Trust," G7 Germany, 2022, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile; "Global Cross-Border Privacy Rules Declaration," US Department of Commerce, last visited September 12, 2022, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

64 All the statistics in this paragraph are from Hamilton and Quinlan, *The Transatlantic Economy 2022*.

Source: European Commission compiled by the Atlantic Council.

States—if the EU's search for digital sovereignty led it to construct barriers against the international digital economy.

As Europe constructs barriers that effectively exclude even its partners from certain elements of the EU tech market and infrastructure, it will create divisions among likeminded democratic states, hindering their ability to better integrate their markets. It will also limit their ability to cooperate in standards-setting bodies and multilateral forums such as the International Telecommunication Union (ITU) and Internet Corporation for Assigned Names and Numbers (ICANN). As a result, the techno-authoritarian governments will have a definite edge, as they seek to dominate the international bodies that manage the Internet and related technology. Perhaps even more important, such divisions among Western democracies will encourage the view in many developing countries that it is better to be aligned with China and Russia.

Because the stakes are so high, the United States and others should respond constructively to the EU's desire for digital sovereignty. The motivation for that approach comes from a very real European problem: the slow development of a local technology environment capable of significant

commercialization of new technologies, and of generating companies on the scale of major US or Chinese digital platforms. Europe also harbors profound concerns about the impact of technology on citizens, leading Brussels to seek to provide protection through comprehensive regulation. Whether the attainment of digital sovereignty will meet those challenges is unclear, but the diagnosis is not without merit. Moreover, it is in the interests of the United States and other likeminded countries that the EU succeed in developing its digital economy and strengthening its technological resilience. All allies and close economic partners would benefit from a stronger EU digital economy that is expanding, becoming more resilient, and bringing new technologies and services to the market.

It is also important to remember that there is not a clear consensus in the EU about digital sovereignty. There are many different definitions of the term, and not all Europeans would agree with the description presented here. Nor do all Europeans even agree about the importance and desirability of digital sovereignty. Many French politicians, for example, would heartily endorse the notion, but across Central Europe and the Nordic states, the focus is more on nurturing their own digital economies and technology centers, and on encouraging the EU to better harmonize digital markets, thereby easing access across the continent for their startups. There are divides as well within the European Commission on how restrictive digital sovereignty should be. As the EU's legislative agenda moves forward, these disparate views of digital sovereignty will continue to fuel debates and different interpretations of law.

Still, the von der Leyen commission has made having an autonomous digital policy a central point of its agenda and its credibility. Debates in the European Parliament have demonstrated that this approach is generally popular; if anything, those parliamentarians critical of commission proposals argue for even stronger rules. And as the EU seeks to strengthen its influence around the world, its digital policy, along with trade, has become a key instrument. In other words, there is little internal incentive for the EU to change course and look for a less expansive approach than digital sovereignty.

European Commission President von der Leyen speaks with French President Macron, US President Biden, and Canadian Prime Minister Trudeau at the G7 Summit in Germany. June 26, 2022. Brendan Smialowski/Pool via REUTERS.

One option for responding to EU measures might be to look for international legal remedies to specific concerns. For example, the French cyber-certification rules and similar proposed EU measures may not be compatible with international trade obligations.[65] Two sets of rules, both promulgated by the World Trade Organization, govern cross-border provision of services: the Government Procurement Agreement (GPA), which addresses government acquisition specifically, and the General Agreement on Trade in Services (GATS), which applies more broadly.

The GPA requires that any state party treat foreign companies supplying cloud services on a cross-border basis no less favorably than locally established suppliers, under the principle of "national treatment." GATS contains similar national treatment commitments, as well as a right to market access in sectors including computer and related services. Both agreements allow exceptions for national security, privacy, and other public-policy interests. There is little WTO precedent in applying these agreements to cloud services, making the outcome of any potential dispute-settlement proceeding highly uncertain.

In considering whether to pursue WTO dispute settlement, the US government is no doubt cognizant that it maintains its own, albeit more limited, restrictions on procuring cloud services. The Department of Defense (DoD), for example, requires that cloud providers keep national security-related data in the United States. However, the DoD requirements do not—in contrast to SecNumCloud or the proposed new ENISA rules—demand foreign ownership be limited to a minority stake as a prerequisite to competing for a defense cloud-computing contract. On September 1, US Trade Representative Katherine Tai raised concerns about the French and EU cybersecurity certification schemes in a call with European Commission Executive Vice President Valdis Dombrovskis, who is responsible for trade–an indication that the issue now has risen to a high level of official concern for the US government.[66]

Other divisions could be ameliorated if the EU and the United States negotiated a bilateral solution to the concerns about the international reach of the US CLOUD that underlie European initiatives such as GAIA-X and cloud cybersecurity certification. Negotiations on an executive agreement on access to electronic evidence began in 2019, but have languished while the EU struggles to enact its counterpart domestic legislation to the CLOUD Act. France made progress on the EU's proposed e-evidence regulation during its recent EU Presidency, making the timing propitious for the Commission to come back to the negotiating table with the United States.

To avoid potential WTO litigation, and in the absence of a bilateral agreement addressing e-evidence issues, the EU should signal willingness to use the Trade and Technology Council (TTC) as a suitable venue for addressing the implications of the EU's digital sovereignty approach and devising transatlantic solutions. Established at the June 2021 US-EU Summit, the TTC is intended to "grow the bilateral trade and investment relationship; to avoid new unnecessary technical barriers to trade; to coordinate, seek common ground, and strengthen global cooperation on technology, digital issues, and supply chains; to support collaborative research and exchanges; to cooperate on compatible and international standards development; to facilitate regulatory policy and enforcement cooperation and, where possible, convergence; to promote innovation and leadership by US and European firms and to strengthen other areas of cooperation."[67] This is an ambitious list of goals, and broad enough to encompass every facet of digital sovereignty, from strengthening European capabilities and creating global standards to ensuring a "level playing field."

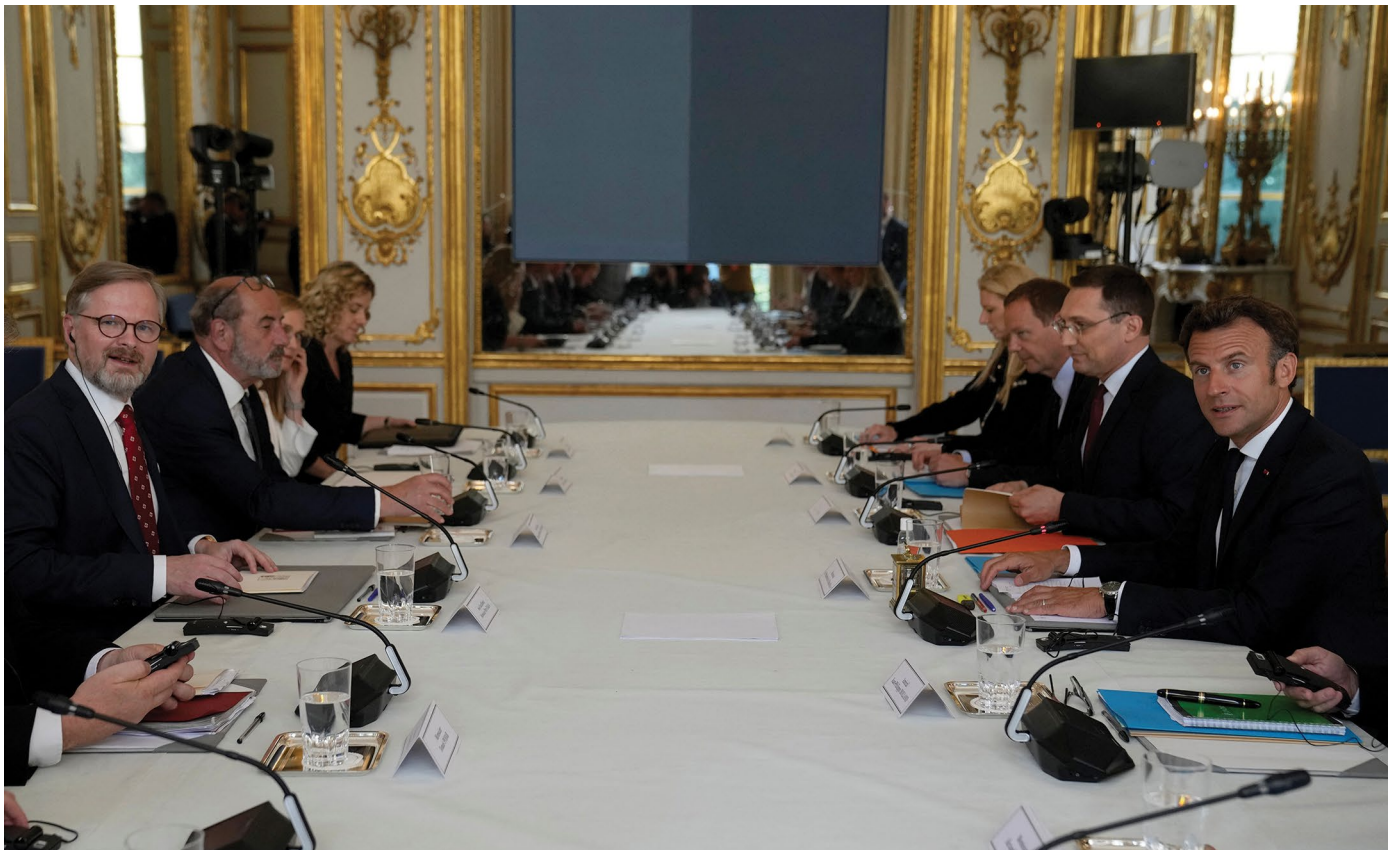
The first two meetings of the TTC, in September 2021 in Pittsburgh and in May 2022 in Paris-Saclay, brought together its co-chairs from the top leadership of the European Commission and US government: US Secretary of State Antony Blinken, Secretary of Commerce Gina Raimondo, US Trade Representative Katherine Tai, European Commission Executive Vice President Margrethe Vestager, and Executive Vice President Valdis Dombrovskis. Perhaps even more important, the TTC established ten working groups across a range of relevant regulatory issues and tasked them with developing collaborative projects. While the actual policy results of the TTC to date have been modest, it does seem to have created a forum for discussion on key issues such as sanctions and export controls.

Although addressing digital sovereignty is not an explicit part of the TTC's mandate, its main goals and working-group structure provide an opportunity for the United States and EU to discuss a wide range of issues and address the tensions around digital sovereignty in the following three areas.

65 Nigel Cory, "'Sovereignty Requirements' in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners," Cross-Border Data Forum, December 10, 2021, https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/.

66 "Dombrovskis, in call with Tai, outlines EU concerns over US EV tax credits, *Inside US Trade*, September 1, 2022, https://insidetrade.com/daily-news/dombrovskis-call-tai-outlines-eu-concerns-over-us-ev-tax-credits.

67 "US-EU Summit Statement," White House, June 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.



Czech Prime Minister Petr Fiala and French President Emmanuel Macron meet at the Elysee Palace, in Paris, France. The Czech Republic brings its own perspective on a vision for Europe's digital future. June 7, 2022. Francois Mori/Pool via REUTERS.

Strengthening transatlantic digital capabilities and resilience. In an effort to boost its technological capabilities, the EU and the US plan to spend billions over the next few years on research and innovation (R&I). Transatlantic research cooperation per se is not addressed by the TTC, as it is covered by the US-EU Agreement for Scientific and Technological Cooperation. However, the TTC clearly intends to foster cooperation on key emerging technologies such as AI, quantum computing, green tech, and telecommunications technologies beyond 5G/6G. The TTC has also facilitated efforts to define key policy elements of technologies, something that will have a strong impact on their widespread adoption. For example, a subgroup of Working Group 1 will develop a joint roadmap on evaluation and measurement tools for trustworthy AI and risk management, while Working Group 2 will work toward aligned approaches for lifecycle assessments of carbon emissions by products, with a long-term goal of encouraging transatlantic convergence on green tech.

Along with facilitating joint research on key technologies, the TTC can help reduce some of the consequences of the EU's emerging industrial policy, including support for such enterprises as GAIA-X and the European Battery Alliance. Both the United States and EU intend to provide financial incentives for semiconductor manufacturers. Working Group 3 is already identifying the information that must be shared to avoid any misunderstandings about specific subsidies, as well as mechanisms for enabling leaders to discuss US and EU subsidies before they escalate. Assuming the United States and EU can develop a shared approach to such subsidies, this effort could usefully be expanded to cover support for other industrial initiatives or to bring in other likeminded jurisdictions, perhaps through the WTO or the G7.

Creating global "gold standards" for regulating tech. EU leaders have repeatedly made clear that they see their domestic rules as suitable for becoming global rules for the digital economy. The size of the European market—four hundred and fifty million consumers—incentivizes many corporations to adopt EU rules as their global norm. A key element of extending EU rules to the global level will be reaching agreement on the standards that form the foundation of these rules, especially on emerging technologies such as AI. If the EU wants to categorize AI according to risk level, for example, there should be international cooperation on common definitions, or at

US Trade Representative Katherine Tai sits with European Commission Executive Vice President Valdis Dombrovskis at a G7 trade summit in London, Britain. October 22, 2021. REUTERS/Henry Nicholls/Pool.

least ways of determining the level of risk. The ongoing efforts of the TTC on this topic are a positive step in this direction.

When it comes to defining actual technical standards for new technologies, the role of international standards organizations (ISOs) will be crucial. Yet both the United States and EU have faltered in their engagement with the ISOs in recent years, leaving them open to dominance by China and other countries with very different ambitions for the global economy. In February 2022, the EU published its own Standardization Strategy focused on the creation of EU-wide standards.[68] At the subsequent Paris-Saclay meeting, the United States and EU established a US-EU Strategic Standardization Information (SSI) mechanism "to enable information-sharing on international standards development," and also promised to "defend our common interests in international standards activities for critical and emerging technologies."[69] Such engagement will be increasingly important if the United States and EU are to build effective collaboration in the ISOs, and could also ensure that EU internal rules are based on a commonly understood foundation. Now is the time for the EU to keep its European Standardization System (ESS) open, inclusive, and consensus-based while seeking alignment with US and international standards.

Examining the European push for localization and, in some cases, discrimination. The TTC could also be an appropriate forum for addressing EU concerns about the vulnerabilities of its digital infrastructure and networks, especially to the actions and laws of other governments. As noted above in the discussions about cloud cybersecurity and transfers of industrial data, too often EU proposals seek to restrict US corporate engagement in Europe, ostensibly because of concerns about US government access to data or the network share held by US firms. Both the Pittsburgh and Paris-Saclay statements made clear that the United States and EU retain their regulatory autonomy, and the formal TTC agenda has shied away from including active disputes or discussions of current legislative proposals. Yet there is no doubt that the TTC offers the opportunity for top leaders to consult informally on common issues such as those relating to data transfers, the pending

68 "New Approach to Enable Global Leadership of EU Standards Promoting Values and a Resilient, Green and Digital Single Market," European Commission, February 2, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661.

69 "US-EU Joint Statement of the Trade and Technology Council," White House, May 16, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf.

implementation of the DMA, the DSA, and the Data Act. In time, such discussions could build confidence for jointly addressing contentious issues.

The TTC could serve as a suitable venue for assessing restrictions on procuring cloud services, for example. One of the goals of WG10 is to share information on "discriminatory treatment of foreign companies and their products and services in support of industrial policy objectives," according to the TTC's inaugural joint declaration.[70] Although this phrase was probably written with China in mind, it provides a potential early-warning opportunity for restrictions in the transatlantic market as well. Alternatively, WG 4 on ICT security and competitiveness could be a suitable forum for discussing how to craft cybersecurity standards without discriminating against non-European providers.

The Paris-Saclay statement also reminds both the United States and EU that they are "trustworthy and reliable trade, technology, and investment partners as well as security partners" who intend "to seek amicable solutions to our differences on trade and to ensure that transatlantic trade flows reflect and promote our many shared interests and values."[71] This spirit was much in evidence during the Paris-Saclay meeting, which came only three months after the Russian invasion of Ukraine. During those months, the United States and EU had developed an unprecedented level of cooperation as they sought to impose sanctions and export controls on Russia.

European Commission Executive Vice President Valdis Dombrovskis, US Trade Representative Katherine Tai, US Commerce Secretary Gina Raimondo, European Commission Executive Vice President Margrethe Vestager, and US Secretary of State Antony Blinken speak with a factory representative during the TTC meeting in Pittsburgh, Pennsylvania. September 30, 2021. Rebecca Droke/Pool via REUTERS.

70 "US-EU Trade and Technology Council Inaugural Joint Statement," White House, September 29, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

71 "US-EU Joint Statement of the Trade and Technology Council," May 16, 2022, Paris-Saclay, France. https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council.

France's Foreign Minister Jean-Yves Le Drian speaks with US Secretary of State Antony Blinken and US Secretary of Commerce Gina Raimondo at the US-EU Trade and Technology Council summit in Paris, France. May 15, 2022. REUTERS/Kevin Lamarque/POOL.

The effort to punish Russia is not limited to Washington and Brussels and EU member states. Several other countries—including the UK, Japan, Australia, South Korea, Canada, and others—joined in those efforts to impose a cost on Russia for its behavior. These likeminded democracies share the values that the United States and EU leaders applaud during TTC meetings.

As major economic partners of the EU, such likeminded countries are also affected by the EU's search for digital sovereignty. While European rhetoric often concentrates on the large US companies, digital sovereignty affects many more countries and their economies. These countries could also be disadvantaged by European ambitions to impose EU rules as global standards, and by the exclusion of companies that are not majority EU owned.

With the reemergence of rival geopolitics and the emergence of a techno-authoritarian view of the digital world, now is an opportune time for the EU, the United States, and likeminded countries to adopt more ambitious shared approaches on digital policy. A first step would be to build on the work of existing multilateral groupings, such as the G7, with its efforts to promote "data free flow with trust," the coalition behind the Declaration for the Future of the Internet, or the Organisation for Economic Co-operation and Development (OECD) Artificial Intelligence Principles. These existing documents set out principles for managing elements of the digital world, and, although largely voluntary and aspirational, they do serve to build consensus about the direction of regulation. Similarly, the TTC, although a bilateral US-EU undertaking, could consciously develop arrangements that are suitable for a broader group of likeminded governments.

But truly solving the issue of conflicting and discriminatory rules for managing technology and the digital economy will require more than a disconnected set of declarations. The United States, the EU, and their partners should seek to align the growing number of such frameworks and develop linkages among them when appropriate. In this way, governments and stakeholders could remove some of the

frictions between national rules. For example, the OECD AI Principles, possibly in combination with the OECD Framework for Classifying AI Systems, may even form the basis for broader plurilateral negotiations that set out in more detail what are acceptable rules and what is discriminatory behavior.

It may even be time for those governments that value an open but trustworthy digital economy to consider a more institutional approach. Just as the countries favoring open and free trade in goods once grouped together to establish the General Agreement on Tariffs and Trade (GATT) and WTO, now may be the time for likeminded "digital democrats" to institutionalize the rules on which they can agree and establish a dispute-settlement process to examine those rules that may be genuinely discriminatory. Just as governments needed to adjust their domestic rules relating to physical goods and services that were found to be contrary to shared trade norms, so a similar system in the digital economy could help remove the friction between different domestic regulatory regimes. This could entail recommitting to the WTO dispute-settlement mechanism, or crafting a plurilateral agreement, initially limited in its number of participants but with a separate dispute-settlement process attached. Even if only initially applicable to a limited number of countries, such an approach could help build the consensus needed to ensure that key parts of the Internet remain free. With time, like the earlier trading system, it may attract many others who are willing to adopt its principles and values.

As the United States considers how best to respond to the EU's search for digital sovereignty, the Biden administration should consider giving greater priority to digital and technology issues on its own agenda. Pushing back effectively against some EU measures—and negotiating with the EU—requires the United States to have a more organized approach than it does currently. US digital policy today largely consists of disparate initiatives on semiconductors, cybersecurity, and competition; the administration has not even indicated support for any of the multiple privacy bills under consideration.

Responsibility for developing a US approach is spread among the White House, Federal Trade Commission, Commerce Department, State Department, Office of the Trade Representative, and other agencies. In contrast, the EU has put forward a more coherent approach, led by one of its highest-ranking officials. Most EU member states have a minister or deputy minister for digitalization who pursues the EU agenda on a national level. Until the United States develops more clarity regarding its own approach to the digital economy, its efforts to dissuade the EU from pursuing a digital sovereignty approach that risks disadvantaging US firms are unlikely to be effective.

The EU's search for digital sovereignty reflects many factors, ranging from Europe's failure to develop truly global digital companies to increasing external threats to the resilience of EU digital infrastructure and services. The United States and other likeminded democracies have an enormous stake in how the EU pursues its vision of digital sovereignty. The last two years have brought greater clarity in the form of legislation and other regulatory measures—and not all of it is good news for the partners of the European Union. No one, including Europe and its citizens, will benefit if the EU proceeds to implement measures resulting in localization and discrimination against non-EU firms. It is time for the EU, the United States, and their partners to discuss this issue frankly and openly, in order to build the stronger cooperation that the current geopolitical world requires.

About the Authors

Frances G. Burwell is a distinguished fellow at the Atlantic Council 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 other most recent report is *Engaging Europe: A Transatlantic Digital Agenda for the Biden Administration*. Among her other publications are: *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 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 2011-2015, he served as Legal Counselor at the US Mission to the European Union, in Brussels, Belgium, 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, US Department of State, Professor 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. Professor Propp holds a J.D. from Harvard Law School and a bachelor's degree from Amherst College. In 2016, he taught European Union law as an adjunct faculty member at George Mason University School of Law.

Acknowledgment

The Atlantic Council's Europe Center would like to thank our sponsors, including Google and Amazon Web Services, for their support of our work.

The Atlantic Council's partners are not responsible for the content of this report, and the Europe Center maintains a strict intellectual independence policy in line with the Atlantic Council Policy on Intellectual Independence.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
*Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members List as of May 2, 2022*

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.

© 2022 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org