Atlantic Council
FUTURE EUROPE INITIATIVE

ISSUE BRIEF

The European Union and the Search for Digital Sovereignty:

Building "Fortress Europe" or Preparing for a New World?

JUNE 2020

FRANCES G. BURWELL AND KENNETH PROPP

The Rise of Digital Sovereignty

When the new European Commission took office under President Ursula von der Leyen, enhancing digital capabilities across the European Union immediately emerged as a top priority. Even in her first statement before being confirmed as European Commission president, von der Leyen called for Europe to achieve "technological sovereignty in some critical technology areas."[1] The German Economy Minister Peter Altmaier also framed this ambition in terms of sovereignty, equating the storage abroad of European data by US cloud-services companies to a loss of sovereignty, while Thierry Breton, in an early statement to the European Parliament as nominee for commissioner for the internal market, called for building Europe's technological sovereignty.[2]

Despite the priority given to technological or digital sovereignty, there was little clear definition of what the term actually means, or even whether digital and technological sovereignty are the same thing.[3] But it was clearly much more than a rhetorical flourish—by March 2020, the European Commission had outlined new legislative proposals covering the development and use of artificial intelligence, the participation of "high-risk" vendors in critical net-

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.

The **Future Europe Initiative** conducts research and uses real-time commentary and analysis to guide the actions and strategy of key transatlantic decision-makers 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.

1 Mark Scott, "What's Driving Europe's New Aggressive Stance on Tech," *Politico*, October 28, 2019, https://www.politico.com/news/2019/10/28/europe-technology-silicon-valley-059988.

2 Javier Espinoza and Sam Fleming, "Europe Urged to Use Industrial Data Trove to Steal March on Rivals," *Financial Times*, January 24, 2019, https://www.ft.com/content/8187a268-3494-11ea-a6d3-9a26f8c3cba4; "Questions to the Commissioner-Designate Thierry Breton," European Commission, 2019, https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf.

3 For the purposes of this paper, the authors distinguish between technological sovereignty, which focuses on infrastructure, innovation, and other technology-driven elements of the digital agenda, and digital sovereignty, which also captures regulatory and policy elements of digitalization more broadly.

"However the EU redefines sovereignty post-COVID-19—including technological or digital sovereignty—the impact will not be limited to Europe and European companies. Indeed, many of these EU initiatives are intended to counter the strong position of US and Chinese digital companies in the European market."

works, and the management of data. At the heart of all these proposals was a desire to strengthen EU competitiveness vis-à-vis dominant players in the digital space, especially the United States and China, while ensuring that the rights of EU citizens are protected. Together, these measures are expected to strengthen EU sovereignty in the digital space.

In March, the COVID-19 pandemic hit Europe full force, and became the dominant issue for both national governments and the European institutions. While the crisis created some delays in the legislative process, it also reinforced the importance of digital policymaking for many Europeans. Individuals found themselves working remotely on platforms with questionable security. Locational data on citizens measured the effectiveness of "social distancing" but raised privacy issues, especially as European governments began to consider the use of contact-tracing apps, and disinformation about the virus was rampant on social media. At the same time, new trade barriers for medical supplies and border closures around the globe—and within the EU—reinforced the need to redefine "sovereignty" in Europe and the world.

However the EU redefines sovereignty post-COVID-19—including technological or digital sovereignty—the impact will not be limited to Europe and European companies. Indeed, many of these EU initiatives are intended to counter the strong position of US and Chinese digital companies in the European market. They will have a significant effect on US companies, and not just on their operations in Europe. Because of the extraterritorial reach of many EU rules, even US companies without a European presence may be affected, as has happened with EU privacy rules.

Given the deep integration of the US and European economies, including their digital economies, this move by Europe could bring serious challenges to the US-EU relationship. The EU clearly has the right to regulate foreign companies, including tech companies, that operate in its market. Its choices about how precisely to regulate in a rapidly innovating and unpredictable economic sector will be key, both for Europe's success and for transatlantic relations. Will the EU's search for digital sovereignty exacerbate regulatory differences between the United States and European Union, perhaps even straying into protectionism? Or will the United States and EU find a way to work together in establishing global norms in the digital space? And, if that fails, will the next few years see the division of the digital world into three spheres: EU, United States, and China?

The Transatlantic Digital Economy

The transatlantic economy is the strongest economic partnership in the world. The United States and the EU are each other's top trading partner and, perhaps more importantly, the top investor in each other's economy. US companies are key actors in the European economy, creating millions of jobs, and vice versa. This is especially true in the digital economy. For both the United States and EU, the leading importer of their digitally enabled services is the other, representing about one-third of their total exports of such services. The US exported $189.9 billion information and communications technology (ICT) and potentially ICT-enabled services to the EU in 2017 and imported $118.1 billion for a surplus of $72 billion[4]. That same year, US corporations, through their local affiliates in Europe, supplied $175 billion in ICT services, while only supplying $3 billion in China and $21 billion in Latin America. It is not surprising that of all US overseas investment in the information industry, 73 percent was in Europe in 2018.[5]

Given this deep interdependence, It is inevitable that the United States and European Union occasionally find them-

4 "International Transactions, International Services, and International Investment Position Tables," Bureau of Economic Analysis, US Department of Commerce, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4#reqid=62&step=9&isuri=1&6210=4.

5 Ibid., 117.

selves in conflict, especially over the growing body of rules governing the digital economy. Following 9/11, new US rules seeking information on travelers collided with EU privacy rules, and there have also been differences over copyright, content, and competition policy. The size of the European market makes it impossible for leading tech and digital companies to ignore. Thus, when the EU passed its General Data Protection Regulation (GDPR), establishing requirements for protection of personal data, many global companies adopted GDPR for all their operations, rather than abandon the European market.

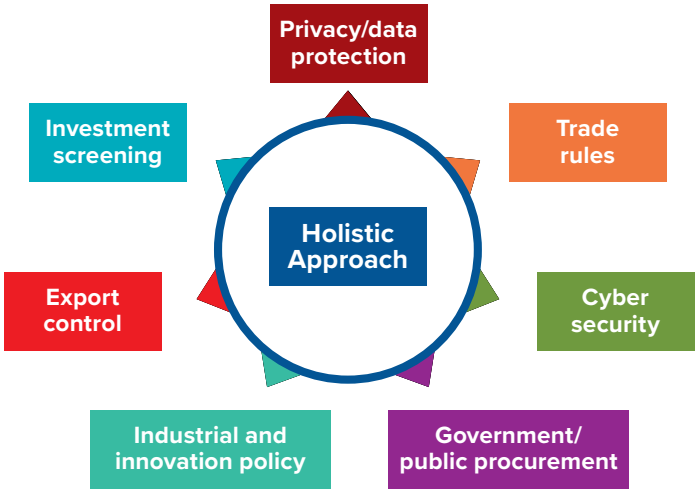
The Drive for European Digital Sovereignty

The current European focus on digital sovereignty has its roots in a much broader discussion about Europe's ability to protect its citizens from an increasingly hostile and challenging world. The financial crisis of 2009–2012, followed by Russian aggression in Ukraine in 2015 and the migration crisis later that same year, led to an awareness of the deterioration in the European Union's external circumstances. The return of geopolitics prompted a review of Europe's strategic position and, at least within EU institutions, gave rise to a belief that Europe should seek greater "strategic autonomy," strengthening its capacity to act externally on its own, especially in the defense realm.[6]

Soon after, US President Donald Trump rocked Europeans' assumptions about their economic security and the steadfastness of the US-EU partnership. In 2018, the United States announced tariffs on steel and aluminum imports, based on national security considerations, and threatened European automakers with similar measures. The US reimposition of sanctions on Iran forced many European businesses to abandon new business ventures and a new market. The US administration also began to reject elements of the multilateral trading system and the World Trade Organization (WTO), threatening the global economic system that Europe saw as fundamental to its own economic success.

China's rapidly increasing investment in key European infrastructure and companies also raised concerns and led to the adoption of EU guidance for investment screening by the member states. In 2019, concerns erupted about the growing role of the Chinese firm Huawei in Europe's new fifth-generation (5G) infrastructure, spurred in part by US pressure. With all these external pressures on the EU economy, the need for Europe to protect its economy from the actions of others—to ensure its economic sovereignty—became a priority topic.[7]

EU outline of policy tools for protecting digital sovereignty



Source: European Political Strategy Centre

In early 2020, the emergence of the COVID-19 virus made even more clear Europe's vulnerability to global disruptions and the actions of others. Industrial supply chains and sources of vital medical equipment were cut off by the impact of the virus and sudden border closures, including within the Schengen area. As governments around the world competed to secure needed equipment, the ideal of a global, open trading system seemed tarnished. For many Europeans, a post-COVID-19 age will require greater security of supply and more government control over those supplies—in short, greater economic sovereignty.

Central to this new world will be an enhanced understanding of sovereignty in the digital sphere. The COVID-19 crisis has made clear the central role digitalization plays in the current world, and its role in responding to a global crisis. The rapid

6 "Shared Vision, Common Action: A Stronger Europe," European Union External Action Service, 2016, https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf.

7 Mark Leonard et al., *Redefining Europe's Economic Sovereignty, Bruegel*, June 25, 2019, https://www.bruegel.org/2019/06/redefining-europes-economic-sovereignty/.

Hearing of Commissioner-designate Thierry Breton, November 14, 2019. *Source:* CC-BY-4.0: © European Union 2019

move of schools, offices, and even social relationships to the virtual world has reinforced awareness of privacy issues and the differences between surveillance measures promoted by China and those acceptable in Europe. Although some social media platforms initially and unwittingly spread false information, they also proved essential for controlling that disinformation.[8] The importance of analyzing massive quantities of health data to track the virus and identify effective mitigation strategies underscores the importance of the new European Commission initiatives on artificial intelligence and data management—including the proposed creation of a health-related data pool.

Before COVID-19, the European debate over digital sovereignty was rooted in a widespread perception that Europe had been disadvantaged by large US tech companies—and, more recently, by Chinese companies—that had come to dominate its market and, in this view, impeded the growth of a European tech sector. Certainly, Europe does not fare well when measured against key tech indicators, and especially considering the size of its market of five hundred million people. While Europe has 387 million Facebook users—compared to 190 million in the United States—no EU company rivals the huge platforms based in the United States.[9] The *Forbes* 2019 list of the top one hundred dig-

8 Mark Scott, "Coronavirus Crisis Shows Big Tech for What It Is—a 21st Century Public Utility," *Politico*, March 25, 2020, https://www.politico.eu/article/coronavirus-big-tech-utility-google-facebook/.

9 "Facebook by the Numbers: Stats, Demographics & Fun Facts," Omnicoreagency, last updated February 10, 2020, https://www.omnicoreagency.com/facebook-statistics/.

ital companies showed only one EU company (Deutsche Telekom) in the top twenty, while US companies claimed twelve spots, China and Japan two each, and Hong Kong, South Korea, and Taiwan one each.[10] Less than 4 percent of the market capitalization of the world's seventy largest platforms is European.[11] In January 2020, Apple alone was valued at $1.42 trillion—more than the entire DAX index of Germany's leading thirty companies.[12]

"While European policymakers can easily find statistics to justify the need for digital sovereignty, they have a much harder time defining that term."

European shortcomings can be attributed in part to regulation, including national barriers that continue to frustrate the achievement of a genuine single market. Varying bankruptcy laws, different capital markets, and different national regulations on robotics, data, and other key elements of a tech economy, all divide the large EU market into multiple smaller national markets, without the scale needed for launching a global tech company such as Google or Facebook. Europe has also suffered from gaps in innovation. While its manufacturing industries have been pathfinders in their own sectors, they have often been slow to adopt digitalization throughout their working methods. European startups have also stumbled when looking for capital to grow their efforts, and often end up relocating to Silicon Valley or being bought out by US firms. In recent calls for digital sovereignty, European leaders have mostly acknowledged these internal shortcomings. Some have also blamed what they see as aggressive market domination by the so-called "GAFA" (Google, Apple, Facebook, and Amazon).

While European policymakers can easily find statistics to justify the need for digital sovereignty, they have a much harder time defining that term.[13] In the most comprehensive effort to identify the components of digital sovereignty, the European Commission's think tank—the European Political Strategy Centre—examined the impact of digitalization on the EU's strategic autonomy and concluded that if the EU wanted to be able to play a role in shaping global affairs, it had to address shortcomings in its industrial and technological base, as well as its critical infrastructure.[14]

Thus, many European officials now think in terms of technological sovereignty and look particularly to the need to grow European capabilities in digital infrastructure, including both networks and cloud services.[15] One early response is the European Battery Alliance, launched in 2017, which brings together the EU institutions with industry stakeholders and innovators, and represents an effort by the European Commission to foster the development of a pan-European battery industry as a strategic imperative.[16] The lack of European cloud services has also received much attention, as has the role of the Chinese company Huawei in 5G networks (see below). This emphasis on technological sovereignty is reinforced by the European Commission's February 2020 proposals on data and artificial intelligence (AI), which stressed the importance of industrial data as a resource on which European experience and innovation could build.

The notion of sovereignty also intersects with the longtime European concerns about privacy and personal data, as well as other key areas on the digital agenda, including taxation, data, and government procurement. As one European Commission paper stated, "Ultimately, the ability of the EU and European stakeholders to shape the rules

10 "Top 100 Digital Companies," *Forbes*, last updated 2019, https://www.forbes.com/top-digital-companies/list/.

11 Anu Bradford, "The Brussels Effect, Continued," *Economist*, February 22, 2020, 63, https://www.economist.com/business/2020/02/20/the-eu-wants-to-set-the-rules-for-the-world-of-technology.

12 Patrick McGee and Guy Chazan, "The Apple Effect: Germany Fears being Left Behind by Big Tech," *Financial Times*, January 29, 2020, https://www.ft.com/content/6f69433a-40f0-11ea-a047-eae9bd51ceba.

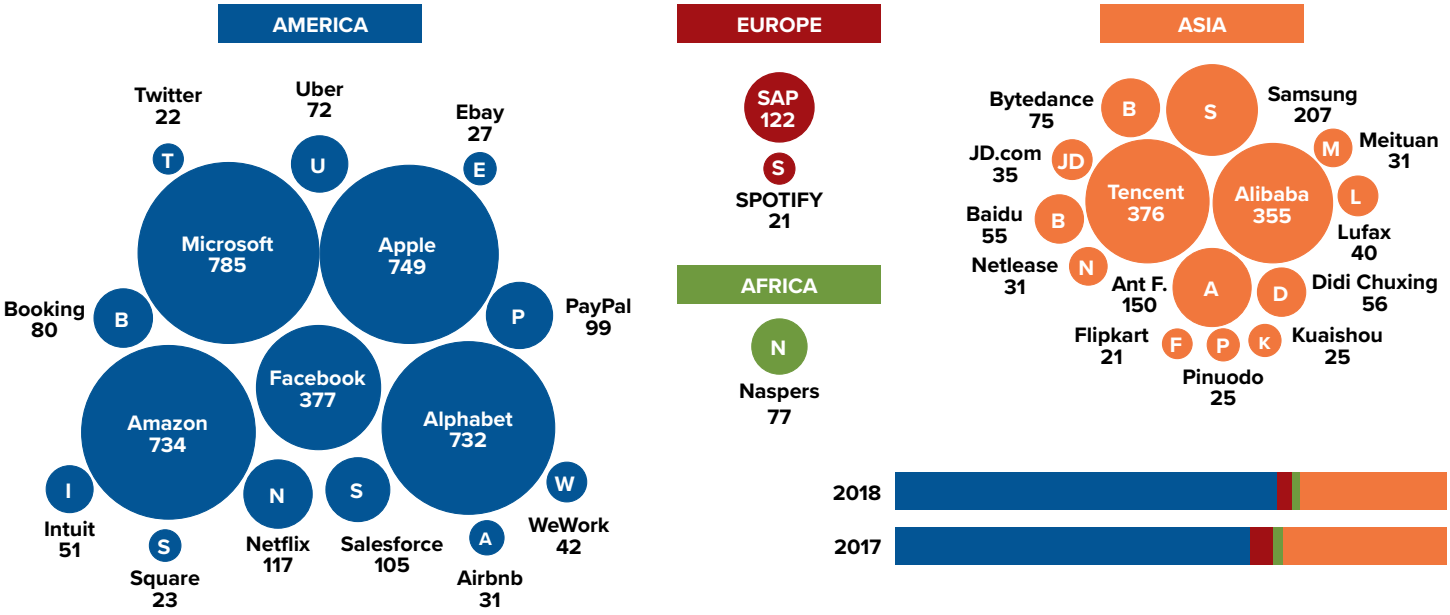
13 Tyson Barker, "Europe Can't Win the Tech War It Just Started," *Foreign Policy*, January 16, 2020, https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/.

14 "Rethinking Strategic Autonomy in the Digital Age," European Commission, last updated July 18, 2019, https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf.

15 Adam Satariano and Monika Pronczuk, "Europe, Overrun by Foreign Tech Giants, Wants to Grow Its Own," *New York Times*, February 19, 2020, https://www.nytimes.com/2020/02/19/business/europe-digital-economy.html.

16 "European Battery Alliance," European Commission, https://ec.europa.eu/growth/industry/policy/european-battery-alliance_en.

Geographical distribution of the main global platforms in the world, 2018, above $20 Billion



Source: United Nations Conference on Trade and Development

and standards governing digital technologies, their use, and the companies producing and operating them, is crucial for its strategic autonomy."[17] Thus, digital sovereignty is a much broader concept, one that includes a strong, innovative industrial base with sufficient cybersecurity protections, but one that also safeguards the ability of the EU to be a "rulemaker" rather than a "rule-taker" when it comes to how digitalization affects its citizens and companies.

As the EU seeks to enhance its digital sovereignty, a key question is whether this effort is essentially protectionist in nature. European officials, of course, deny any such tendency: in response to a parliamentary questionnaire, then-Commissioner-designate Breton stated, "This is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent."[18] On other occasions, however, he has said that his ambition "is that European data will be used for European companies in priority, for us to create value in Europe."[19] The key question will be whether European rules—including the many new digital regulations expected to be adopted in the next two years—will treat European companies more favorably than non-EU companies, and so effectively discriminate against the latter. Clearly, there are voices in Europe who favor such a course of action, including breaking up large non-EU tech companies or banning them from certain markets.[20] Even within the European Commission, there are differing voices, with Breton emphasizing the need for EU companies to be among the top digital leaders, but Executive Vice President Margarethe Vestager arguing that companies must compete within Europe if they are to succeed in global competition.

17 "Rethinking Strategic Autonomy in the Digital Age," European Commission.

18 "Questions to the Commissioner-Designate Thierry Breton," European Commission.

19 Janosch Delcker "Thierry Breton: European Companies Must Be Ones Profiting from European Data," *Politico*, January 19, 2020, https://www.politico.eu/article/thierry-breton-european-companies-must-be-ones-profiting-from-european-data/.

20 Foo Yun Chee, "EU's Vestager Says Breaking Up Companies is Last Option," Reuters, October 8, 2019, https://www.reuters.com/article/us-eu-antitrust-vestager/eus-vestager-says-breaking-up-companies-is-last-option-idUSKBN1WN1PS.

"Whether Europe's search for digital sovereignty will turn into 'Fortress Europe' will depend on what happens in key sectors of the digital economy."

Whether Europe's search for digital sovereignty will turn into "Fortress Europe" will depend on what happens in key sectors of the digital economy.

Government Procurement and 5G Infrastructure

European governments, especially in Germany, have already started to place restrictions on the national origins of the hardware, software, and digital services they purchase, often citing a sovereignty justification. An early instance occurred in 2014, when the German government cancelled a contract with Verizon, a US company, to supply telecommunications services to a number of German federal agencies. The government cited concerns—in the immediate wake of the Edward Snowden revelations about National Security Agency (NSA) surveillance activities—that US intelligence agencies could demand that Verizon provide them access to stored data relating to Germans. More recently, some German state governments have decided not to utilize foreign software in processing public data. Microsoft, for example, has lost contracts for the use of its Office 365 software program in schools in Hesse, after concerns were voiced by the state's data protection authority that the company would use student data for its own internal business purposes.[21]

Increasingly, Germany is casting its federal software-procurement policies in the blunt language of sovereignty. In September 2019, Interior Minister Horst Seehofer emphasized the finding of a commissioned report on "digital sovereignty in public administration" that German government agencies were increasingly dependent on standardized software products from a few foreign companies.[22] "In order to safeguard our digital sovereignty," he asserted, "we will reduce dependency on individual IT providers, as well as review alternative programs to replace specific software."[23] The German government stated that it would toughen conditions of use in software procurement contracts and rely more on open-source software, adding that it would be acting in close coordination with the EU.

By far the starkest transatlantic tension in the government-procurement area is the ongoing controversy over the purchase of Chinese components produced by Huawei and, to a lesser extent, ZTE for use in 5G telecommunications networks. The United States has taken the maximalist position that any Huawei participation in US 5G networks would risk penetration by Chinese intelligence. The United States also lobbied European governments at the highest levels to follow its lead in excluding Huawei from participating in 5G upgrades to their own telecommunications systems. Reportedly, it went so far as to threaten the United Kingdom with a cut-off in intelligence sharing through the Five Eyes network if it chose to purchase from Huawei. The UK, however, took a middle course, opting to purchase Huawei components for incorporation only in peripheral, less sensitive parts of its 5G networks. France and the Netherlands also have adopted this posture. In Germany, a decision has been delayed due to disagreement within the CDU/CSU parties.

Although the EU lacks competence to harmonize member-state procurement decisions, the European Commission in early 2020 issued a communication on 5G deployment setting out a recommended approach similar to the UK's. While avoiding specific mention of China, it urges member states to assess the risks that particular vendors may pose, including the location of their headquarters, surveillance laws with which they must comply, and any judicial possibilities for challenging surveillance requests. The European Commission calls on member states to exclude high-risk vendors from critical or sensitive parts of their 5G networks, including the Internet backbone and core networks that manage data traffic.[24] The EU's increased sensitivity to

21 Kenneth Propp, "Waving the Flag of Digital Soverignty," Atlantic Council, December 11, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/.

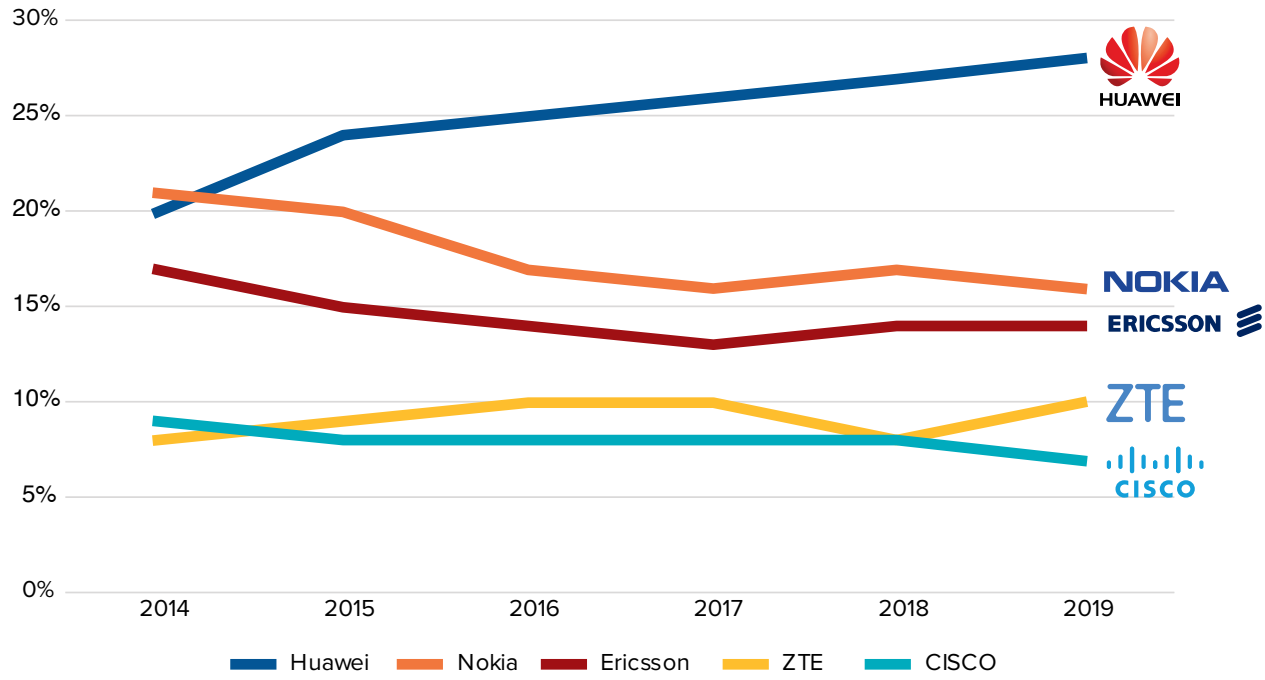
22 "Dependency on Individual Software Providers: Strategic Market Analysis, Final Report," PricewaterhouseCoopers, August 2019, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse_en.pdf?__blob=publicationFile.

23 Propp, "Waving the Flag of Digital Sovereignty."

24 Laurens Cerulus, "Europe's Huawei Plan Explained," *Politico*, January 29, 2020, https://www.politico.eu/article/europe-eu-huawei-5g-china-cybersecurity-toolbox-explained/.

China's Growing Dominance in Service Provider Equipment

By share of Revenue on the Worldwide Telecom Equipment Market



Source: Dell'Oro Group

the risks of 5G technology is thematically consistent with its 2019 legislation establishing a framework for national-security-based screening of incoming foreign investment, akin to the US law enhancing screening by the Committee on Foreign Investment in the United States (CFIUS).

European governments have diverged from the United States on procurement from Huawei primarily because of the higher costs they would incur by choosing other suppliers, and because Huawei is already a supplier in many of their less sophisticated telecoms networks. Ironically, the market participants that would benefit most from excluding Huawei are two prominent European companies, Ericsson and Nokia. In this case, the desire for European digital sovereignty conflicts with the understandable tendency to opt for the less expensive alternative.

Cloud Computing: European Champions and the Road to Data Localization?

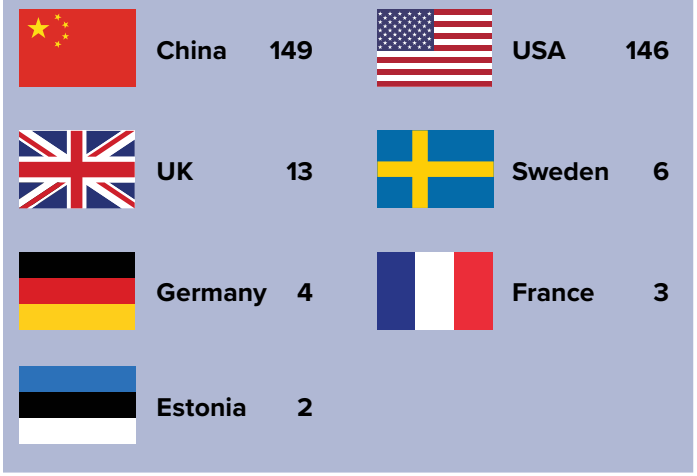
Cloud services are an essential part of any modern digital infrastructure. US companies currently supply the overwhelming share of cloud-computing services used in Europe, with 92 percent of the Western world's data stored in the United States. US-based Amazon Web Services has one third of the global market for hosting corporate data, with Microsoft and Google following with 16 percent and 7.8 percent of the market, respectively.[25] In response to this situation, the European Commission's *Communication on a European Strategy for Data* establishes as an EU priority to "reduce its technological dependencies" in cloud infrastructure and services, in part through EU funding of a "federated cloud infrastructure."[26] It promises to contribute two billion euros to the cause, with member states and indus-

25 Propp, *Waving the Flag of Digital Sovereignty*.

26 "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions," European Commission, February 19, 2020, 9, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

try kicking in additional funds to reach a total of four to six billion euros to establish "EU-wide common, interoperable data spaces" in strategic sectors.[27]

Total number of 'Unicorn' Start-ups (valued above $1 billion), by country, 2018



Source: www.nanalyze.com

France and Germany have already set off down this path, independently of the EU. In October 2019, the two governments, in conjunction with national industrial companies, announced GAIA-X, a project to connect cloud providers around Europe. It would use open technical standards and shared data privacy and security standards so that businesses and customers could move industrial data around freely within the network. In February, the two governments issued a paper that made clear their political ambition: "In order to gain sustainable digital sovereignty, it is important to strengthen Europe's competitiveness in the global digital market."[28] The paper proclaims, "Data sovereignty 'by design' will be a guiding principle for the development of software for platforms and services."[29] Intergovernmental discussions about the organization and governance of GAIA-X are now underway, while industry representatives are collaborating on the technical aspects. France and Germany are approaching other governments to join this binational venture, while the commission proposes to "foster synergies" between its work on a European cloud federation and member-state initiatives such as GAIA-X.[30]

By building European cloud services, European governments seek to keep in Europe data generated on the continent, in part to protect that information from non-European governments. The GAIA-X paper notes, "Protection against abuse of national regulations that allow access to data stored in cloud infrastructures or services is an essential part of the European federated data infrastructure."[31] The European Commission's data strategy makes the same point, observing that the US CLOUD Act "raises legitimate concerns for European businesses, citizens and public authorities over legal uncertainty and compliance with applicable EU law, such as data protection rules."[32] It goes on to encourage conclusion of a US-EU CLOUD Act agreement—negotiation of which is now under way—as a way to resolve this potential conflict.[33]

Many EU member states have taken a further step against what is seen as US sovereign encroachment by enacting "data localization" measures that preclude certain categories of data from being relocated outside their territory. Data localization measures exist across Europe, including in Belgium, Bulgaria, France, Germany, Greece, Luxembourg, the Netherlands, Poland, Romania, and Sweden. Typically,

27 Ibid.

28 "Germany, France Sign Common Paper to Support European Cloud Infrastructure Gaia-X," *Telecom Paper*, last updated February 20, 2020, https://www.telecompaper.com/news/germany-france-sign-common-paper-to-support-european-cloud-infrastructure-gaia-x--1327334.

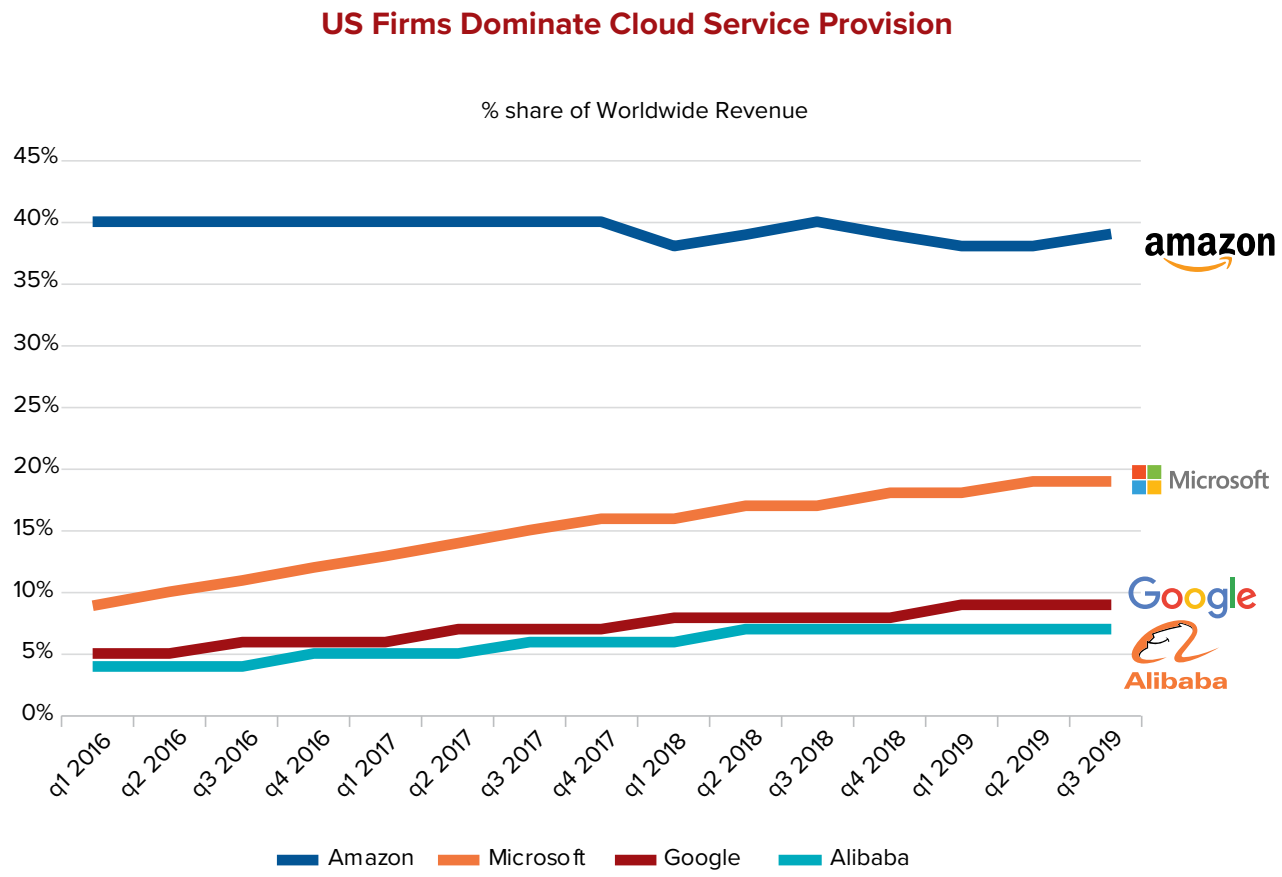
29 Ibid.

30 "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions," 18.

31 "Germany, France Sign Common Paper to Support European Cloud Infrastructure Gaia-X," 2. German tech entrepreneurs have eagerly echoed this rhetoric, with the director of Owncloud demanding that "Europe finally grow up and free itself from dependency on the American internet giants and the chokehold of the US CLOUD Act." (Tobias Gerlinger, "Corona Makes It Crystal-clear: We Urgently Need a European Data Infrastructure," *ECIN Technik & Business Praxiswissen*, March 25, 2020.)

32 The 2018 CLOUD Act provides that a US court may require an Internet platform with a US presence to produce a customer's personal information for use in a US criminal investigation or prosecution—even if the data are held on a foreign server. The law thereby mooted a case then pending before the US Supreme Court in which Microsoft had questioned the extraterritorial scope of a US warrant used to obtain electronic evidence abroad.

33 "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions," 9. The CLOUD Act also authorizes the US government to negotiate international agreements for the production of electronic evidence. In 2019, the United Kingdom became the first country to conclude such an agreement with the United States.



Source: Synergy Research Group

they apply to a particularly sensitive type of data, such as health-related personal data or data used in a particular business sector, such as financial services.[34]

There can be legitimate public policy motivations for some data-localization measures, of course. A national bank regulator may reasonably assert a need for local financial institutions' information to be stored in its territory, so that it would be available for urgent review in the event of a bank failure, for example. However, data localization can also be used for less salutary aims, such as ensuring a market for local cloud-service providers, even if they offer fewer services and less security.

The EU's comprehensive privacy law, the GDPR, does not preclude member states from enacting localization measures for personal data, although it does create a framework for international data transfers generally. On the other hand, the EU has acted decisively to bar most localization measures within the EU for non-personal data. Such data are particularly crucial to the industrial internet (or "the Internet of Things"), as data from sensors are constantly used for a range of business purposes, including the improvement of machines' performance. In 2018, the EU adopted a regulation to assure the free flow of non-personal data within the EU by prohibiting localization, unless a national measure is justified on grounds of public security.[35]

34 Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost*, Information Technology & Innovation Foundation, May 2017, Appendix A, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.63382255.1306428313.1587045825-1501175350.1587045825.

35 Framework for the Free Flow of Non-personal Data in the European Union of the European Parliament and of the Council of 14 November 2018, Regulation 2018/1807, Article 4 (2018).

Member states have until 2021 to repeal existing measures or to attempt to justify them to the European Commission.

Some governments, including the United States and Asian leaders like Japan, have turned to trade agreements as a tool for limiting the extent to which localization measures may be employed against their companies. The US-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement both set out clear limits for localization measures affecting personal data. Japan failed to persuade the EU to address data flows in their 2019 Economic Partnership Agreement, securing only a promise to revisit the issue in several years.

Data and Artificial Intelligence: The Lifeblood of Digital Sovereignty

Following the worldwide proliferation of cloud computing, the latest dramatic data advance is AI—a collection of technologies, such as machine learning, that combine data, algorithms, and computing power to yield insights of value to business, government, and consumers. The new European Commission is determined that Europe not miss an opportunity for global prominence in developing AI, as it is widely considered to have done in the case of cloud computing. "The winners of today will not necessarily be the winners of tomorrow," it defiantly asserts in its "European Strategy for Data," issued in February.

AI technology uses sophisticated algorithms to analyze pools of data, and the European Commission intends that within ten years, "the EU's share of the data economy—data stored, processed and put to valuable use in Europe—at least corresponds to its economic weight, not by *fiat* but by choice." The data strategy aims to create "a single European data space," a single market where business has access to a rich pool of non-personal, as well as personal, data drawn from a variety of sources. Creating such a data space "in turn will increase Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy," such as big-data analytics and machine learning. In the United States, by contrast, "the organization of the data space is left to the private sector, with considerable concentration effects," the European Commission avers. It is equally dismissive of China's approach, marred by "a combination of government surveillance" with corporate control over data "without sufficient safeguards for individuals."

The European Commission, in conjunction with issuing its data strategy, also published its *White Paper on Artificial Intelligence*, sketching out the key elements of a regulatory regime tailored to this new technological phenomenon. Projected EU legislation would harmonize divergent regulatory approaches to AI now appearing in member states; take a risk-based, sector-specific approach; identify high-risk sectors and applications, including facial-recognition software; and impose testing requirements to ensure that high-risk AI systems conform to requirements for safety, fairness, and data protection before they are released onto the market.[36] This initial approach appears to be nuanced and modest, but much will depend on how the rules evolve during the legislative process.

Digital Taxation: A Sovereign Right?

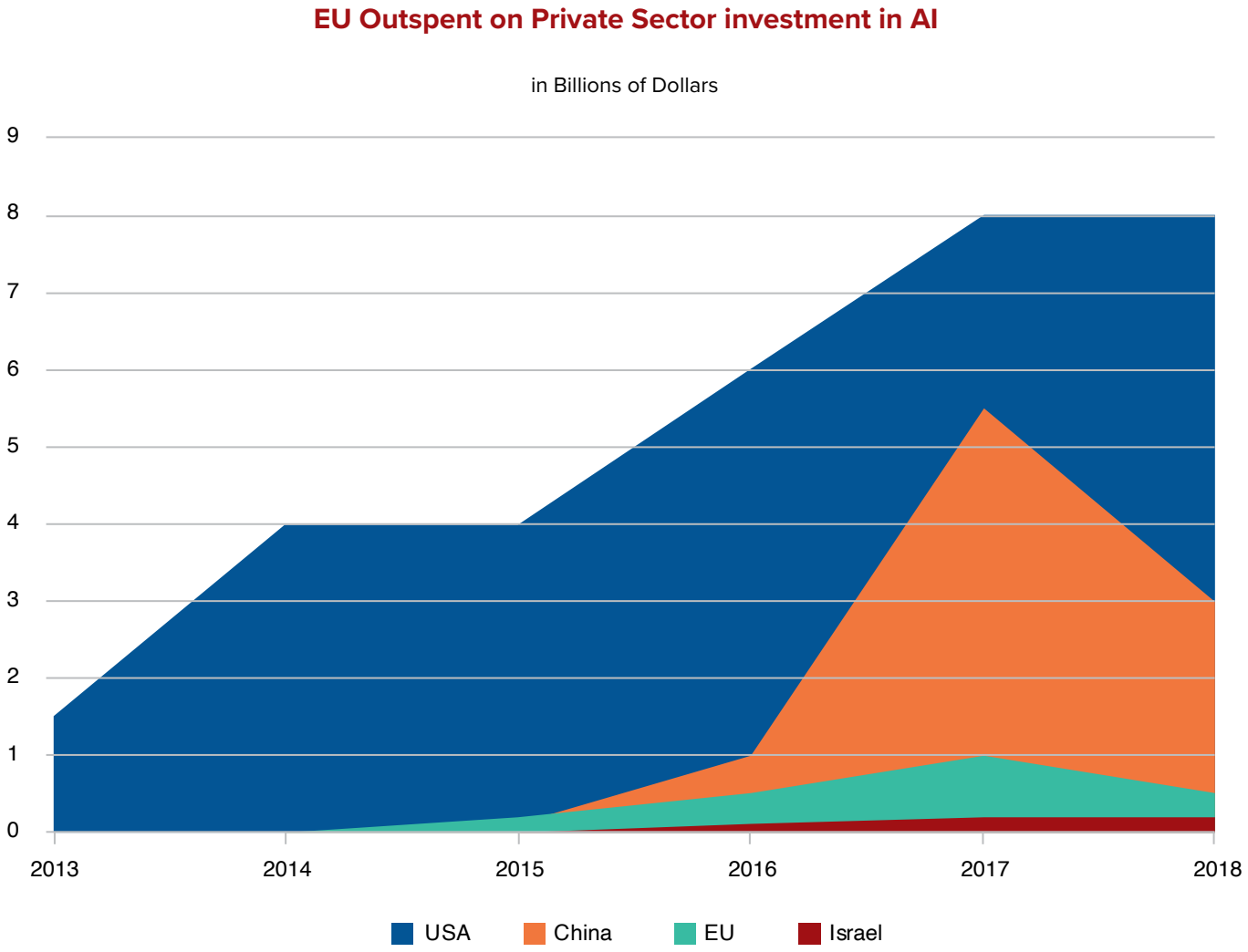
Nothing is more sovereign than the imposition of tax, and taxation of companies supplying digital services has recently emerged as a particularly intense area of transatlantic conflict. The traditionally high-tax continental European jurisdictions have long harbored resentment that US digital-services companies not only dominate their domestic markets, but also pay comparatively lower rates of corporate tax than those paid by local companies in traditional industries.[37] A contributing factor is that digital companies may derive revenues through interactions with users in jurisdictions where they may not have the physical presence that usually triggers local taxability. This combination of foreign companies dominating digital-service markets and the inability of European governments to tax them at levels according to local sensibilities is highly combustible.

In 2018, France spearheaded an effort to have the EU create a digital services tax (DST), but a number of lower-tax member states—including Ireland, Sweden, and Denmark—objected, dooming the initiative.[38] France responded to

36 Mark MacCarthy and Kenneth Propp, "The EU's White Paper on AI: A Thoughtful and Balanced Way Forward," *Lawfare Blog*, March 5, 2020, https://www.lawfareblog.com/eus-white-paper-ai-thoughtful-and-balanced-way-forward.

37 There is disagreement on exactly how much less tax US digital services companies pay. A 2018 European Commission report stated that digital services companies pay up to 14 percent less effective overall tax, but the Office of the US Trade Representative (USTR) disputes that figure. ("Section 301 Investigation: France's Digital Services Tax," US Trade Representative, last updated December 2, 2019, 5, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-frances-digital-services-tax).

38 The EU may only adopt harmonized tax measures if member states unanimously agree. (Treaty on the Functioning of the European Union, TFEU, Article 113 (1957)).



Source: Organisation for Economic Co-operation and Development

the defeat at the EU level by adopting a national-level digital services tax, which took effect in January 2020. The French measure imposes a three percent tax on the gross turnover of digital platforms that offer advertisements (such as Facebook or Google), that intermediate the sale of services (like Uber or Airbnb), or that sell user data.[39] Only platforms that generate more than seven hundred and fifty million euros in global taxable digital services and twenty-five million euros in France are subject to the DST, leading many to conclude that it is targeted primarily at the large US-based platforms. Other European countries have since followed France's lead, including Austria, Hungary, Italy, and the United Kingdom, and still others are considering a DST.

The fact that the French tax falls almost exclusively upon US digital services companies has predictably led to a sharp reaction from the US government. In December 2019, the Office of the US Trade Representative released a report finding the French DST to be discriminatory, setting the stage for the imposition of retaliatory tariffs under

39 E-commerce platforms like Amazon, or content providers such as Netflix, are not subject to the French DST.

President Donald J. Trump meets with French President Emmanuel Macron in London, England, on December 3, 2019. *Source:* State Department Photo by Ron Przysucha

Section 301 of the Trade Act of 1974.[40] The White House quickly announced that tariffs on up to $2.4 billion of French goods were being considered. However, in January 2020, Presidents Donald Trump and Macron agreed that France would forbear from collecting the tax this year and the United States would defer imposition of tariffs.

Key to the Franco-American entente was a renewed commitment by both sides to the ongoing multilateral tax negotiation at the Organisation for Economic Cooperation and Development (OECD), which is scheduled to be concluded in late 2020. One hundred and thirty-seven countries have participated in the work of the OECD/Group of Twenty (G20) Inclusive Framework on Base Erosion and Profit-Sharing (BEPS). This initiative aims to agree on a global approach to calculating how tax should be imposed on companies that conduct economic activity in a jurisdiction where they do not have a traditional physical presence. The BEPS effort may also establish a minimum corporate tax rate in order to deter profit shifting to lower-tax jurisdictions.

Success in the OECD negotiations this year is far from guaranteed. Failure could have significant consequences in the form of a re-escalation of sovereign conflict. European Commission President von der Leyen has already pledged to introduce new EU tax legislation if the OECD does not

40 "Section 301 Investigation: France's Digital Services Tax," 1.

reach agreement by the end of 2020. Inevitably, more EU member states would adopt digital services taxes while waiting for the EU rules to take shape. And, in all likelihood, the US government would impose increased tariffs on European goods, leading to broader transatlantic tensions.

Privacy: The Original European Push for Digital Sovereignty

Europe's privacy activists have long invoked the need for sovereignty, although they define it less in terms of European industry and more as a reassertion of the individual's ability to control what happens to personal data in the hands of companies or governments. This political impulse powered the passage of the GDPR in 2016. With strict requirements for consent and limits on the permissible use of personal data, the GDPR is a vindication of Europeans' fundamental right to privacy protection.

But the GDPR goes even further—by controlling the movement of personal data from Europe to other jurisdictions, the GDPR provides an ambitious example of the EU's exercise of sovereignty in the digital space. A company may only transfer data outside EU territory if it puts legal arrangements in place to ensure that the data will enjoy privacy protection in the destination country equivalent to that within the EU. In other words, the EU demands that, when European-origin data travel, the EU's internal privacy rules must be respected extraterritorially. The one exception is an acknowledgement that a foreign sovereign may demand data from a company and supervene these privacy protections when national security requires.[41]

Even before the GDPR became effective in May 2018, the United States and the EU had clashed over their competing assertions of sovereignty over privacy and national security. After Edward Snowden's disclosure of widespread US electronic surveillance of Europeans, Max Schrems, a young Austrian privacy activist, challenged the European Commission's finding that US privacy guarantees for Europeans' data, contained in the Safe Harbor Framework, should still be regarded as "adequate." In 2015, the European Court of Justice (ECJ) agreed that widespread US surveillance effectively invalidated the Safe Harbor Framework. The United States and the European Commission patched together a successor agreement, the Privacy Shield, that carefully describes the limits in US law on foreign surveillance, and that allows Europeans some modest additional procedural protections. European privacy activists promptly sued in the ECJ to have Privacy Shield invalidated, while Max Schrems asked the ECJ to invalidate another mechanism of ensuring privacy protections—the standard contract clauses. The court is expected to rule in both cases later this year, and its judgments could profoundly unsettle transatlantic digital commerce.[42]

The clearest evidence of the GDPR's sovereign ambition is its "blocking" provision. Article 48 forbids companies operating in the EU from complying with a unilateral third-country demand for data, whether it be for national security or law-enforcement reasons. Only requests made pursuant to international agreements, such as mutual legal assistance treaties, may be honored. This provision was unofficially dubbed the "anti-FISA clause" during the drafting of the GDPR, and indeed the United States government heatedly—and unsuccessfully—objected to it. It has not generated direct conflicts between European and foreign sovereigns so far, although companies remain concerned that they may be caught in the middle of future disagreements.

Even as the United States and EU negotiate a transatlantic CLOUD Act agreement to address this conflict, some EU member states have sought in their own way to resist the long arm of US law enforcement demands for electronic evidence. In France, a government commission has issued a report (the Gauvain report) that recommends strengthening and expanding the scope of the country's existing—but largely unused—blocking statute to prevent corporate compliance with foreign data requests.[43] In Sweden, a government digitalization organization, eSam, has ruled that outsourcing public-sector data to US cloud-service providers subject to the CLOUD Act would violate Sweden's law on access to information and secrecy.[44]

41 The EU-US Privacy Shield Principles provide that privacy protections "may be limited....to the extent necessary to meet national security....requirements," ("Overview," Privacy Shield Framework, February 23, 2016, paragraph 5, https://www.privacyshield.gov/article?id=OVERVIEW.)

42 Kenneth Propp, *Putting Privacy Limits on National Security Mass Surveillance: The European Court of Justice Intervenes,* Atlantic Council, February 21, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/putting-privacy-limits-on-national-security-mass-surveillance-the-european-court-of-justice-intervenes/.

43 Propp, *Waving the Flag of Digital Sovereignty*.

44 Ibid.

EU Digital Sovereignty: Panacea or Problem?

As Europe embarks on a wide-ranging quest for greater digital sovereignty, does the experience of GDPR offer any indication of how Europe might seek to operationalize and enforce sovereignty in the digital world? Will the EU seek to protect European industrial or health data in the same way it has sought to protect European personal data around the world? Clearly, there are indications that its forthcoming rules for management of data and AI may have extraterritorial reach, potentially restricting the export of European data unless the other jurisdiction has adequate safeguards. And taxation, unless coordinated through the OECD or similar institutions, clearly has the potential for conflicts over which government has the right to tax specific income. Many governments—including the United States—put restrictions on government procurement or infrastructure investments, using sovereignty and the domestic economy as the rationale, but tensions in this area are also increasing.

> "Whether digital sovereignty will be the panacea that many in the EU seem to hope for is far from clear."

Whether digital sovereignty will be the panacea that many in the EU seem to hope for is far from clear. The European Commission has proposed a number of practical measures aimed at boosting the EU's capabilities, such as targeted funding for research and innovation; digital-skills education for citizens; and support for both startups and the industrial mainstays of the European economy. The new COVID-19 economic recovery plan advanced by the European Commission prioritizes spending on digital and environmental projects. Assuming no state-aid strictures are violated, these are positive steps. These measures alone will not resolve the fundamental challenges that Europe faces as it seeks to build its digital capabilities. In particular, the EU needs to create a genuine digital single market, a project that is underway, but that does not yet allow EU companies to scale up to a continental market. Financing and the availability of capital will also be key, but the EU effort to create a capital markets union has largely stalled.

The European Commission is in the process of developing an extensive digital regulatory framework, one that its supporters believe would protect European citizens from the excesses of the digital world and allow Europe to brand its digital sector as the most human-centric and ethical in the world. But that emerging regulatory framework will also make the European digital sector a more managed economic space. Depending on the final shape of that regulatory regime, and its ability to provide the flexibility required for the rapidly evolving technology sector, it may leave less room for the innovation and scalability that Europe's digital economy needs.[45] The next year will be crucial, as European Commission thinking is turned into specific legislative proposals and advances toward enactment. These new rules will probably not be as harmful and restrictive as some may fear, although there is no doubt that the pandemic has provided an extra impetus for those arguing for sovereignty. But neither are they likely to be transformational for European digital capabilities: they may make Europe more sovereign in the nominal sense of establishing rules for European data, but they will not make Europe a global leader in data.

The push for digital sovereignty will inevitably have an impact on the transatlantic partnership. EU leaders, including Commission President von der Leyen and Commissioner Breton, have committed to creating a "level playing field" for European companies, but have not adequately defined this term or said how the field would be leveled. Will this require taking steps against the US and Chinese companies that dominate European digital life? Or will building up European companies in some way be sufficient? Will rules be written in such a way that they effectively discriminate against US companies? Talk of the "level playing field" can only increase concern on the US side, while encouraging member states and members of the European Parliament (MEPs) to look for ways to limit the opportunities available to non-EU companies.

The European debate over digital sovereignty and its various elements has arisen at a time of high tension in the US-EU relationship. Many in the US foreign policy community have resented the EU adoption of "strategic autonomy" as an ambition in and of itself. "Digital sovereignty" elic-

45 Frances G. Burwell, *First Privacy, Now Data: The EU Seeks a Managed Digital Space,* Atlantic Council, March 3, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/first-privacy-now-data-the-eu-seeks-a-managed-digital-space/.

its some of the same concerns: Sovereignty from whom? Sovereignty how?

After three years of rising tensions with the Trump administration, particularly in the sphere of trade and economics, few European governments are willing to curtail EU ambitions because of US concerns. Criticizing the United States and its role in Europe's digital economy has unfortunately become good politics in many areas of Europe. The experience of the COVID-19 response has only increased the distrust of the Trump administration among European leaders. If the pandemic has generally increased awareness about the importance of the digital sector of the economy, it has also made any reliance on US policy and technology even more suspect.

If the United States and European Union continue to move in separate, and potentially conflicting, directions in the digital sphere, the country that will benefit most is China. Already a massive digital market, with leading global companies such as Tencent and AliBaba, China takes a distinctly different view of digital regulation, ranging from state aid to privacy. Moreover, China's surge of new investments in Europe during the past decade, both in the digital economy and infrastructure, makes clear its ambition to be a global player. Its headline-grabbing public diplomacy during the COVID-19 experience and willingness to employ disinformation have shown a darker side of that ambition.

The United States and the European Union must face this challenge together. They should be working together on a broad array of digital policy issues to ensure that their approaches to the digital economy—and not China's—become the global norms. COVID-19 will undoubtedly spur both the United States and EU to focus on ensuring that key elements of their economies—including the digital sector—are resilient to foreign manipulation and domination. However, this should not mean excluding any foreign participation or erecting barriers in the global economy. Instead, the United States and the European Union should work to create standards and rules in the digital space (as well as in the traditional economy) that reflect their values and interests. As the EU moves forward with new regulatory initiatives, it is the optimum time for the United States and EU to begin identifying shared perspectives and objectives.

There are modest but tangible ways for the United States and the European Union to mitigate their growing digital divergence. Digital policy issues presented by cybersecurity (including vis-à-vis the Internet of Things), artificial intelligence, disinformation, and other emerging digital technologies and practices are ripe for transatlantic dialogue. Such cooperation is also the best way of ensuring that the EU move toward digital sovereignty is genuinely focused on enhancing Europe's own capabilities rather than excluding others. Europe's path forward in the digital arena is not yet set—it is time for both the United States and the EU to make the right choices as they prepare for a new digital, post-COVID-19 age.

Frances G. Burwell *is a distinguished fellow at the Atlantic Council and a senior adviser at McLarty Associates. She directs the Atlantic Council's Transatlantic Digital Marketplace Initiative and, until January 2017, served as vice president for European Union and Special Initiatives. Her work focuses on the European Union and US-EU relations as well as a range of transatlantic economic, political, and defense issues.*

Kenneth Propp *is an international lawyer who served as legal counselor at the US Mission to the European Union from 2011-15. He teaches European Union law at Georgetown University Law Center. He is a non-resident senior fellow with the Future Europe Initiative at the Atlantic Council.*

The Future Europe Initiative thanks Google for its generous support of our work.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

CHAIRMAN EMERITUS
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
Matthew C. Bernstein
*Rafic A. Bizri
Dennis C. Blair
Linden Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Ronald M. Freeman
Courtney Geduldig
Robert S. Gelbard
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mian M. Mansha
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
*Kostas Pantazopoulos
Carlos Pascual
W. DeVier Pierson
Alan Pellegrini
David H. Petraeus
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Mary Streett
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
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
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

List as of May 15, 2020

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

Atlantic Council

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

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