

Go to the Mattresses: It's Time to Reset U.S.-EU Tech and Trade Relations

ROBERT D. ATKINSON | OCTOBER 2024

In its bid for tech sovereignty, the EU has been aggressively targeting U.S. firms and industries with unfair protectionist policies. This cannot stand. To move forward into a new era of deeper transatlantic trade integration, America must first demand a level playing field.

KEY TAKEAWAYS

- The EU's trade surplus with America is more than \$200 billion. Yet it targets U.S. firms with a raft of discriminatory regulations, purchasing policies, and protectionist measures that both extract revenue from and reduce revenue to U.S. industries.
- Left unchecked, Europe's approach provides a protectionist model for other countries and regions to emulate, which would fragment the global digital economy into national and regional "walled gardens."
- U.S. officials have complained diplomatically instead of "going to the mattresses," because the Washington policy community argues the transatlantic U.S.-EU partnership is critical for broader strategic interests. But that approach hasn't worked.
- Congress and the next administration should review of U.S. trade tools and develop new reciprocal measures to counter the EU's digital protectionism and tech sovereignty.
- Offensive measures could include updating Section 301 of the Trade Act to address digital trade, using ICT service reviews against European firms, imposing mirror taxes to offset the EU's digital service taxes, and limiting U.S. data flows to the EU.
- Defensive measures could include limiting federal procurement opportunities, scrutinizing critical exports, excluding EU firms from the U.S. defense industrial base, and retaliating against hypocritical standards for government access to data.
- Ultimately, these measures should be in the service of putting in place a world-class EU-U.S. trade and technology agreement.

CONTENTS

- Key Takeaways 1
- Introduction 3
- EU-U.S. Relations in the Era of China and “Tech Sovereignty” 5
- Europe’s Trade Surplus With the United States 7
- The Bill of Particulars: How Europe Unfairly Targets U.S. Industry 11
 - Discriminatory Purchasing 12
 - Consumer Purchases 12
 - Commercial Purchases..... 13
 - Government Purchases..... 13
 - Extracting Revenue From the United States 13
 - Digital Service Taxes 13
 - Exorbitant Fines 14
 - Network Usage Fees 15
 - Reducing Revenue to the United States 15
 - Price Controls on Drugs..... 15
 - Open Source Technologies 15
 - Discriminatory Regulations 15
 - Digital Markets Act and Digital Services Act Discrimination..... 16
 - Restrictions on Data Flows 16
 - Import Substitution of U.S. Cloud Services..... 17
 - Arbitrary Privacy Enforcement..... 18
 - Standards..... 19
 - Weaponized Antitrust..... 20
- Menu of Options 20
 - Offensive Trade Policy Options 21
 - Amend, and Use, Section 301 to Target Digital Trade Issues 21
 - Pursue a Section 301 Investigation of the DMA and Other Digital Sovereignty Initiatives 21
 - Use Department of Commerce ICT Service Reviews to Cover EU Firms 22
 - Impose Mirror Taxes on Countries That Impose Digital Service Taxes..... 22
 - Create a Cause of Action Allowing U.S. Firms to Sue for DMA-Mandated Disclosure of Trade Secrets and Confidential Information 22
 - Limit Transfers of U.S. Citizens’ Data to the EU..... 23

Defensive Domestic Economic Tools	23
Limit Federal Procurement Opportunities for EU Firms	23
Scrutinize Critical Exports to the EU by Removing Their “Favorable” Designation	23
Exclude EU Firms From the U.S. Defense Industrial Base	23
Retaliate Against Hypocritical Standards for Government Access to Data and Surveillance.....	24
The EU and the China: Brothers in Arms?	25
But Wait, Isn’t the United States Protectionist?	26
Regaining Atlanticism for the China Era	27
Conclusion	27
Endnotes	29

INTRODUCTION

After the United States saved Europe from a Nazi takeover and then for 45 years shielded it from a Soviet invasion, most European policymakers embraced “Atlantic Europe”: a view that Europe needed to be closely tied to the United States, both economically and militarily. But with the fall of the Soviet empire, Europe turned inward to construct a single integrated European Market (EC-92). Now that this project has largely been completed, Europe is shifting to “Fortress Europe,” seeing China and the United States as almost equivalent techno-economic challengers, focusing on technological sovereignty vis-à-vis America while taking a “get as much as you can” approach to trade with China.¹ Many European leaders still want the protection of Pax America, but the leeway to attack U.S. firms and the U.S. economy, and the freedom to engage freely with the Chinese economy—including by selling products to China that the United States forbids with export controls. It is time for the United States to say enough is enough. In doing so, the goal should not be to separate from Europe, but rather to create a more level playing field that enables a new era of deeper integration, grounded ideally in a comprehensive and bold EU-U.S. trade agreement.

Europe is making a strategic mistake of untold magnitude by abandoning Atlantic Europe in favor of Fortress Europe. It would be akin—to use a *Lord of the Rings* analogy—to Rohan deciding that both Gondor and Sauron posed equal risks. China is just too powerful, and its technological, military, and economic progress are so rapid that if the EU continues to try to go it alone, China will surely succeed in its divide-and-conquer strategy.

However, it would be a mistake for U.S. policymakers to be so desperate for transatlantic concord that they continue to downplay the EU’s techno-economic aggression. It’s time for America to start pushing back by making it clear Europe does not get a free ride in attacking U.S. techno-economic interests while making its own side deals with China.

U.S. policymakers must do more than complain diplomatically to French, German, and other EU policymakers in various dialogues and fora about their efforts to replace goods and services from

U.S. tech firms. If the United States tried something similar in a sector in which European firms held most of the market—such as luxury vehicles—the righteous outcry from European defenders of the rules-based global trading system would be immediate and damning. Yet, because European leaders drape their efforts in “European values” and associated privacy, competition, and cybersecurity interests, U.S. policymakers and the media give them a free pass. Even when European leaders repeatedly and consistently say the quiet part out loud—that they want to replace U.S. firms and products—U.S. policymakers still pretend that European partners are acting in good faith, or that they don’t really mean it.

Encouraging Europe to change its approach to U.S. tech has geostrategic implications. Europe is in a different place strategically in relation to China than it was just five years ago. Europe and many other Western nations, such as Australia, Canada, New Zealand, and South Korea, would like nothing more than to see the Chinese mercantilist “cat” belled, but they all lack the courage to do it. So, Europe is happy to leave that task to the United States—describing the conflict wrongly as the U.S.-China trade war—so they can avoid punitive retaliation, while at the same time enabling their companies to take U.S. market share in China. Indeed, that is exactly what has happened. While the United States has been taking the heat in fighting back against Chinese innovation mercantilism—a task that benefits Europe perhaps even more than it does America—the EU has moved in and captured what was formerly U.S. market share there.² That is not how an ally behaves.

The EU needs to join with the United States to limit China’s techno-economic aggression, and at the same time cease its own aggression against the United States.

Europe is still largely anchored to policies of the past in thinking that it can appease China and maintain its market access, and China won’t eventually target its advanced industries for eradication. European officials often talk in private about concerns they share with the United States about China, but the time for subtlety and inaction has long since passed, because the United States no longer has the ability on its own to potentially force change in China. That time is long past. It will take a concerted and coordinated effort for the United States, Europe, Japan, Australia, Canada, South Korea, and other allies to have any chance of enacting collective defenses against predatory Chinese economic practices. A united front can impose costs on China that together would have the potential to limit its gains in advanced industry market share.

So, the EU needs to join with the United States to limit China’s techno-economic aggression, and at the same time cease its own aggression against the United States. But the United States has not established any real policy to make the EU think there could be tangible consequences for its discriminatory policies. U.S. officials’ approach has been to complain to their European counterparts, not “go to the mattresses,” largely because the U.S.-European policy community argues that America needs the EU for broader strategic interests, especially resisting Russian aggression. While President Trump (and other past U.S. presidents, such as Kennedy) have focused on the threat of withdrawing troops, Europe has always known that was a paper tiger.³ And so it has proceeded apace.

It’s time for the United States to respond more strategically. Just as the EU seeks to add new instruments to its strategic autonomy toolbox to ensure it can defend itself against countries that

abuse its openness—from a carbon border adjustment mechanism (CBAM) to mirror clausesto anticoercion instruments—so too must the United States.⁴ Congress and the next administration should review U.S. trade defense tools to reflect the rise of European protectionism and digital sovereignty. If left unchecked, Europe’s approach will provide a model for other countries and regions to emulate, which ultimately will lead to the fragmentation of the global digital economy into national and regional “walled gardens.”

The first part of this report provides current and historical context and examples of EU “tech sovereignty” and tech protectionism to highlight that, while not new, it presents a strategic threat to U.S. trade and tech leadership, especially in light of Chinese techno-economic aggression. The second part details the large EU trade surplus with America. The third part details the EU’s array of unfair “innovation mercantilist” practices and policies. The final part puts forth ideas for new, reciprocal tools the United States can develop and use against European firms, technologies, and trade to demand a level playing field.

EU-U.S. RELATIONS IN THE ERA OF CHINA AND “TECH SOVEREIGNTY”

The transatlantic relationship appeared to get back on track in 2021, with the United States and Europe having put aside disputes over the Airbus-Boeing file (although Airbus had benefited vastly more from its subsidies than Boeing did from its) as well as the steel and aluminum dispute; they also launched the EU-U.S. Trade and Technology Council to engage in dialogue on a range of tech issues. However, these papered over even deeper trade conflicts, including in digital industries. There is a clear synergy between the European Commission’s industrial and trade policy strategies, but just not in the open and fair way that Europe so often likes to portray itself in the context of “defending” the rules-based international trading system. U.S. policymakers need to realize that this is neither incidental nor accidental. In fact, it’s central to their approach. The United States needs to treat it as such, similar to how it treats Chinese protectionism.

European policymakers commonly portray digital and tech sovereignty as a strong yet nebulous concept, usually referring to the assertion of state control over data, data flows, and digital technologies, coupled with the replacement of U.S. technology firms with European ones. That it helps them “take back control” and “sovereignty” from mainly U.S. technology firms is not a bug, but rather a central feature.⁵ The European Center for International Political Economy has summarized the mix of four factors behind the emergence of technological sovereignty: culture, control, competitiveness, and cybersecurity.⁶ In reality, there is only one: protectionism.

While the vague and broad notion about state “control” over data and digital technologies is evident in the various policy issues and debates, it is clear what this means in practice: targeting U.S. firms and products to ultimately replace them with European ones. European leaders such as former German chancellor Merkel and French president Macron explicitly have called for both digital protectionism and data sovereignty in talking about digital and technological sovereignty.⁷ It means different things to different officials.⁸ For example, the mere fact that data from companies such as Volkswagen were stored on Microsoft and Amazon servers was enough for Germany’s former economy minister Peter Altmaier to state that “in this we are losing part of our sovereignty.”⁹ The French minister for economic affairs went so far as to call U.S. “big tech” companies “adversar[ies] of the state.”¹⁰

For the European Commission, European control largely means that Europe’s policymakers retain the capacity to cater to European firms and advance Europe’s economic interests globally.¹¹ Ursula von der Leyen, the European Commission president, signaled the EU’s protectionist objectives: “We must have mastery and ownership of key technologies in Europe.”¹² Sabine Weyand, the Commission’s director-general for trade, has echoed that point, arguing there has been a shift in the international order from a rules-based system to a power-based system, and the EU has every interest in opposing that shift because rules-bound international trade protects everyone from arbitrary discrimination.¹³ To that end, Weyand says Europe needs to proceed with what she calls a “dual integration” of everything the EU does economically at the international level on one hand, and on the other hand internal EU policies such as industrial policy, internal market policy, competition, or even research policy.¹⁴ In sum, Weyand says, “we must accept this duality, whereby we continue to defend a multilateral order based on rules, but also accept that it is essential that the EU do so from a stronger position.”¹⁵ While European officials defend their conceptualization of “open strategic autonomy” as not being about autarky and self-sufficiency, at every turn when it comes to tech policy, that’s exactly what it is.¹⁶ Even if Ms. Weyand doesn’t interpret it this way, other European officials and political leaders are enacting digital regulations that ultimately reflect this.

Even the recent Draghi report on EU competitiveness reflects this view, even if it often uses code words to mask the EU’s intentions. But with regard to cloud computing, the intent is open: “For reasons of European sovereignty, the EU should ensure that it has a competitive domestic industry that can meet the demand for ‘sovereign cloud solutions.’”¹⁷

European efforts to undermine American tech leadership and firms are not new, but simply the latest in a long history. Likewise, so is American concern about how to respond. Three quotes from the 1960s reflect this historical point:

He who has technological superiority is master.... [U.S. dominance] risks creating a science gap to the benefit of the United States ... a loss of balance from which our economic freedom of action could suffer.... He who has technological superiority is master.... Certainly it would be absurd to systematically oppose oneself to the introduction into a country of a foreign firm which brings in a superior technology and thus contributes to economic progress.... Nevertheless, we do not see how a Nation could maintain its political independence if such penetration becomes generalized.¹⁸

- P. Cognard, France’s Délégation Générale à la Recherche Scientifique et Technique (1964)

To assist [Europe’s] process by a technological subsidy ... might serve to perpetuate bad European practices. Moreover, a substantial part of our favorable trade balance depends on our tech superiority & we should not give it away for nothing.¹⁹

- Telegram from the Department of State to Secretary of State Rusk (1966)

Political concern in Europe with the technological gap remains high.... They recognize that all of the major factors are ones they must deal with themselves, and there is no longer talk of a ‘Marshall Plan for technology.’ But a deep

uneasiness remains ... we encountered evidence of rising nationalism everywhere, most clearly in Germany, where the view was expressed, for example, that a major modern State must have an independent capacity to produce computers which are the key to the new society of the electronic age ... the fear within Europe of U.S. domination in key European industries is a source of political strain.... Europeans are anxious to benefit the maximum extent from U.S. technological advances while avoiding possibility of American tech domination. This combination of aims has resulted in an ambivalent approach. On the one hand, they are considering essentially protective measures. On the other, they would like the broadest access to US gov-financed R&D.²⁰

- Memorandum from the President’s Special Assistant for Science and Technology (Hornig) to President Johnson (1967)

While Europe targeted U.S. firms and trade during the Cold War, the strategic context was clearly different, including the overarching emphasis on “Atlanticism.” Europe depended almost completely on the United States to keep it from being invaded by the Soviets. Today, while Russia is a security issue for Europe, it’s not an existential-level threat. Nor is it something that, if Europe had bothered to build up its own military, Europe could not today handle on its own.

Europe also benefited technologically and economically from U.S. military protection. As the new Draghi report on EU competitiveness notes, “The safety of the US security umbrella freed up defence budgets to spend on other priorities. In a world of stable geopolitics, we had no reason to be concerned about rising dependencies on countries we expected to remain our friends.”²¹ It was not the United States that said no to friendship; it was Europe. And there is no word of thanks here; no acknowledgment that the fact that the EU could and did scrimp on defense spending enabled it to spend on commercial technology development at the cost of the United States.

Also, during the Cold War, Europe was not a serious threat to U.S. technological leadership, so it didn’t pose a strategic risk. However, now it is different, and with U.S. (and European) advanced industries under threat from China, the United States cannot afford two-front techno-economic aggression. The Cold War is over, and Europe’s discriminatory tech policies can and do have a sizable impact on U.S. tech firms and their hard-fought leadership positions.

EUROPE’S TRADE SURPLUS WITH THE UNITED STATES

Listening to European policymakers and politicians target U.S. tech firms and products, one might be excused for thinking that the EU must be running massive trade deficits with the United States that are hollowing out its economy. The reality is completely the opposite. In 2023, the EU ran a trade surplus of \$208.7 billion with the United States (figure 1). As seen in figure 2, the EU runs significant trade surpluses with the United States in pharmaceuticals and medical devices, motor vehicles and parts, electrical goods, telecommunication goods, chemicals, and instruments. Of the 27 EU nations, all but 7 (Malta, Luxemburg, Croatia, Lithuania, Belgium, Spain, and the Netherlands) runs trade surpluses in goods with the United States. And the country whose officials complain the loudest of U.S. “digital dominance”—Germany—runs the largest trade surplus.²²

Figure 1: U.S. trade deficit with the EU (billions)²³

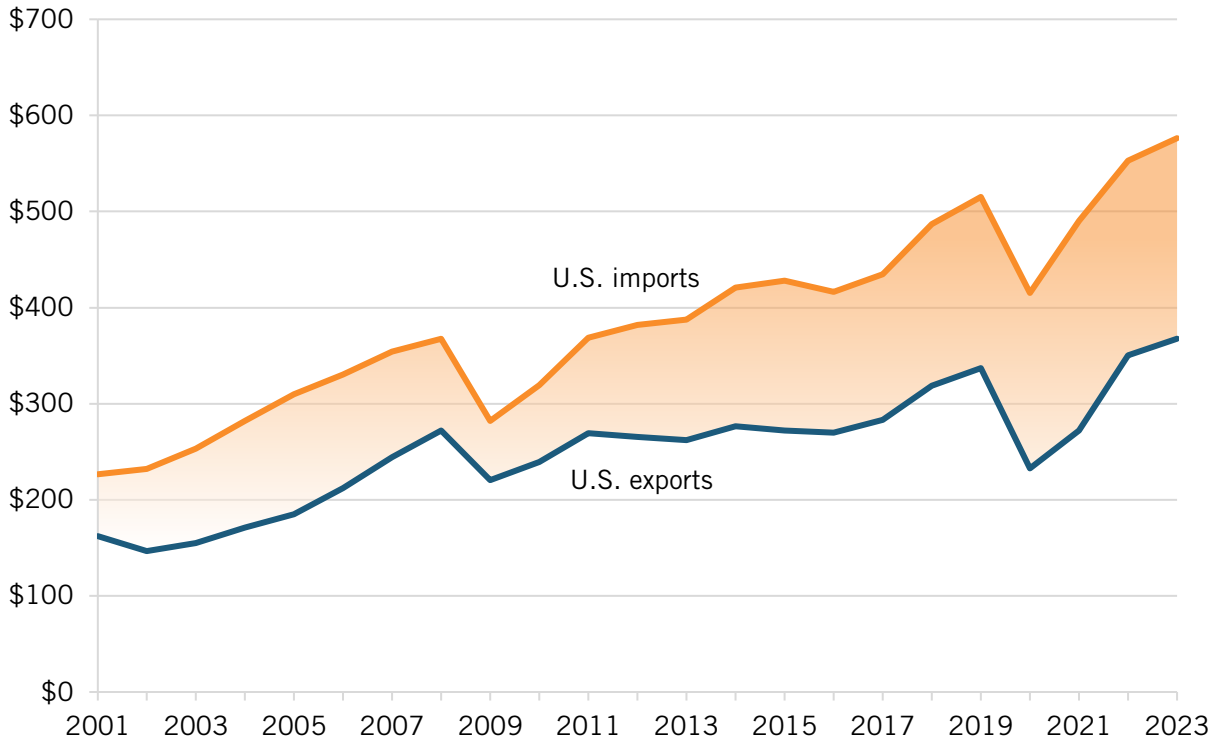
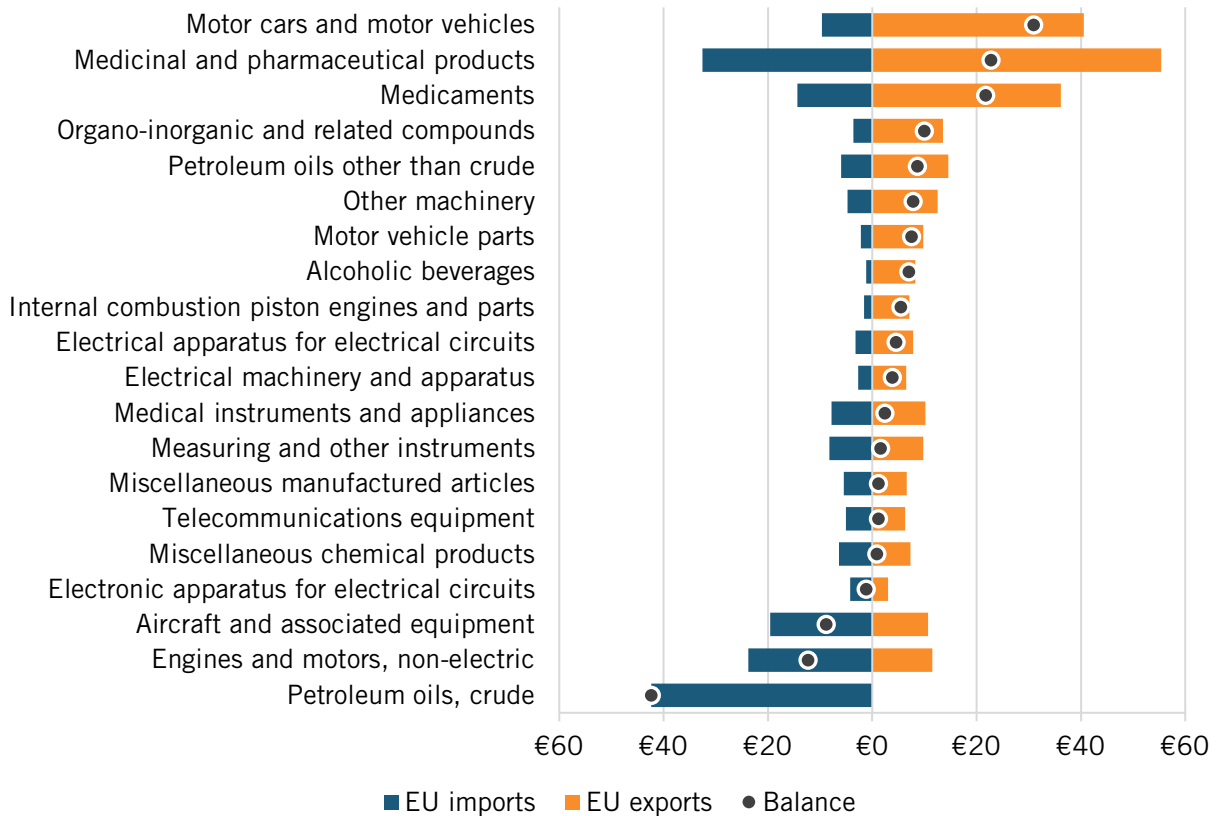


Figure 2: EU trade balance with the United States in goods industries, 2023 (billions)²⁴



As figure 3 and figure 4 show, the EU has a large and growing surplus in trade in two key categories: automobiles and pharmaceuticals.

Figure 3: U.S. trade deficit with the EU in automobiles (billions)²⁵

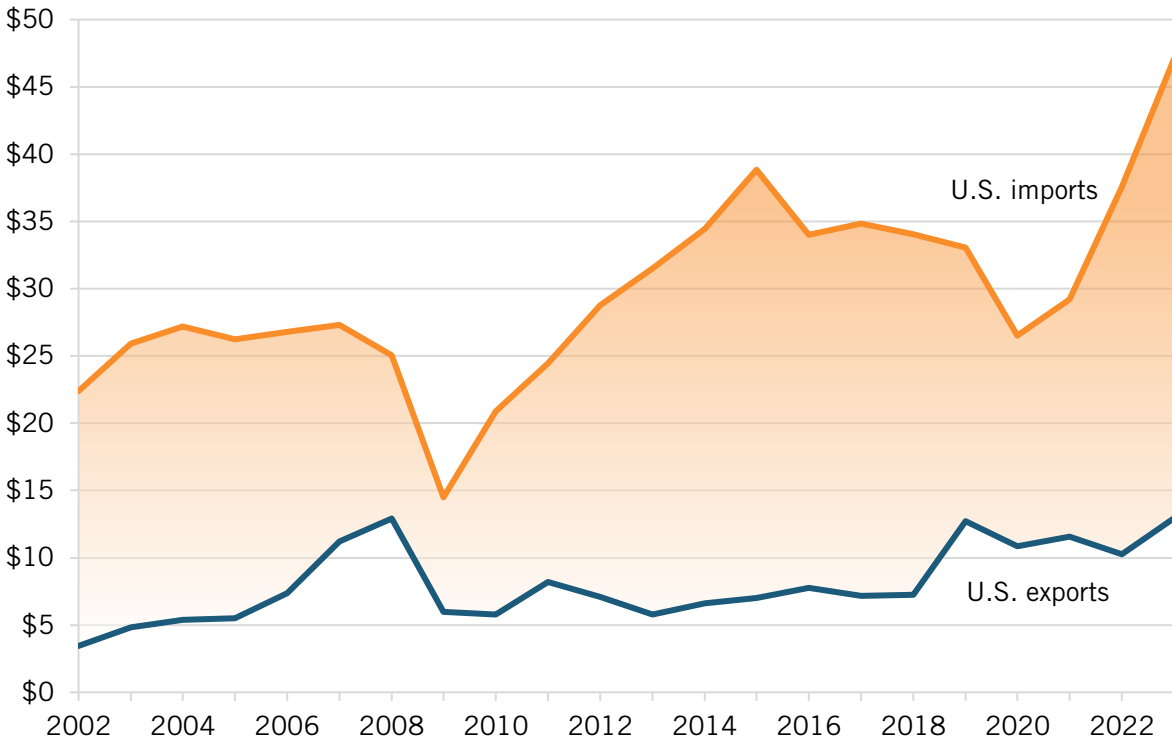
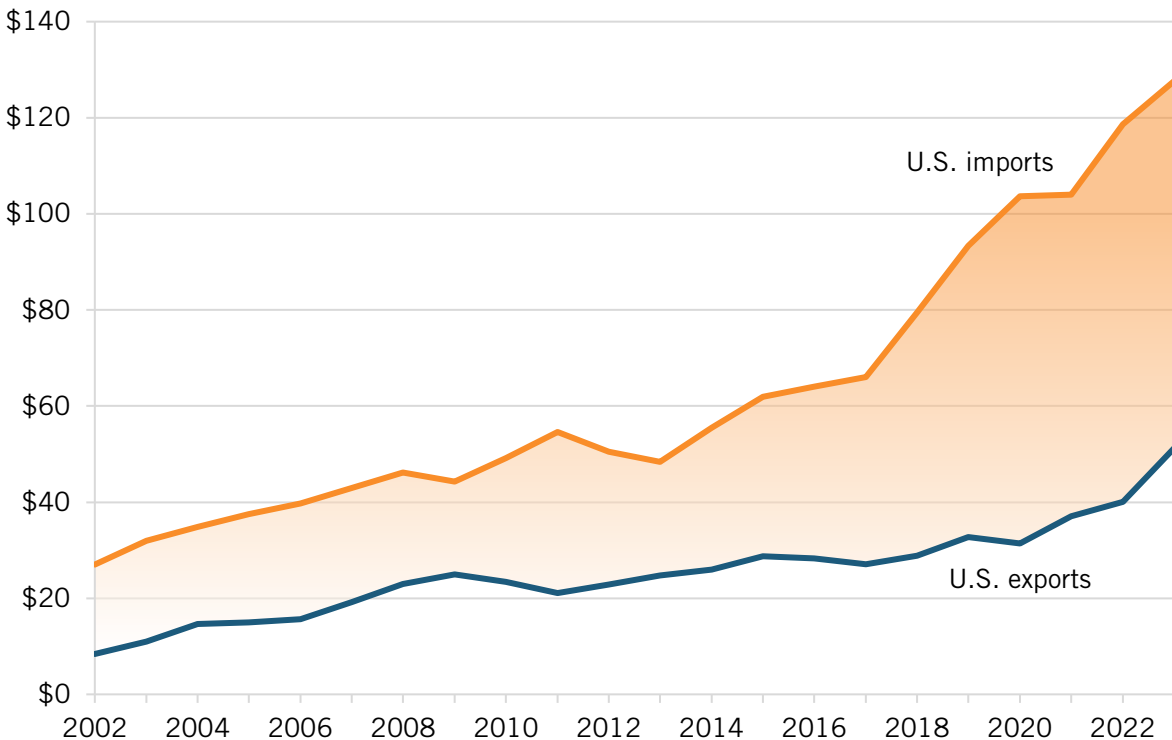
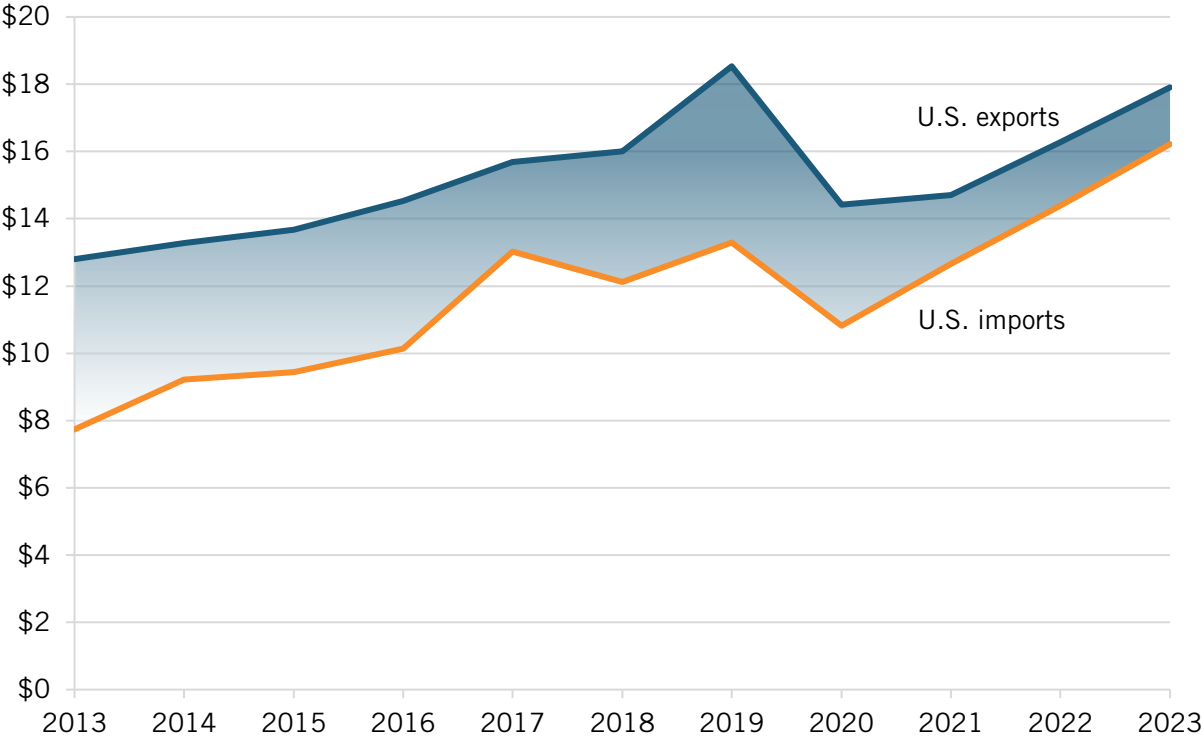


Figure 4: U.S. trade deficit with the EU in pharmaceuticals (billions)²⁶



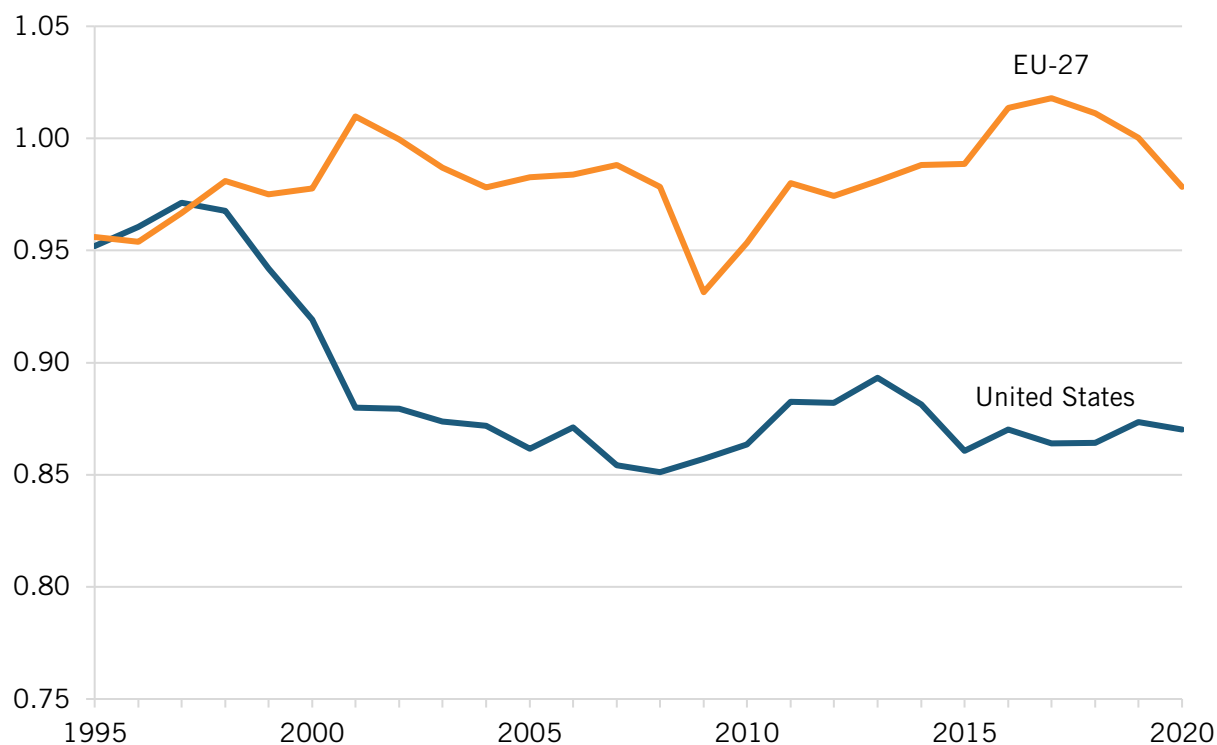
In one of the few areas where the U.S. runs a surplus—digital services—the EU is trying to undermine it. Analyzing the International Monetary Fund’s (IMF’s) “telecommunications, computer, and information services” category in the Balance of Payments guide is a readily comparable measure of digital services across countries. The telecommunications, computer, and information services trade category captures the trade of services included in the broadcast or transmission of sound, images, data, or other information by electronic means, hardware and software, and database services and web search portals, among other services.²⁷ It shows that transatlantic trade is large and growing, while the U.S. trade surplus in these services is shrinking. U.S. digital services exports to the EU rose from \$12.8 billion to \$17.9 billion between 2013 and 2023, while EU digital services exports to the United States rose from \$7.7 billion to \$16.2 billion. (See figure 5.)

Figure 5: U.S. trade surplus with the EU in telecommunications, computer, and information services (billions)²⁸



The EU is also outperforming the United States in relative performance in the 10 Hamilton Industries: pharmaceuticals; electrical equipment; machinery and equipment; motor vehicle equipment; other transport equipment; computers, electronic, and optical products; information technology and information services; chemicals; basic metals; and fabricated metals. Relative performance is measured using a location quotient (LQ), which is a measure of industrial specialization relative to the rest of the world. An LQ of 1 means a country’s share of global output in an industry is on par with the size of the global average. Since 1998, the EU’s LQ has exceeded the United States’ rather steadily. (See figure 6.) As of 2020, the LQ of the EU was 0.98 and the United States’ LQ was 0.87, meaning that, while the EU has been able to produce and grow in these strategically important sectors at a pace almost equal to the global average, the United States has fallen behind.

Figure 6: Relative performance (LQ) in the advanced industries included in ITIF's Hamilton Index²⁹



THE BILL OF PARTICULARS: HOW EUROPE UNFAIRLY TARGETS U.S. INDUSTRY

There are a host of ways Europe protects its markets and attacks U.S. competitors, all of which contribute to the large bilateral trade imbalance.

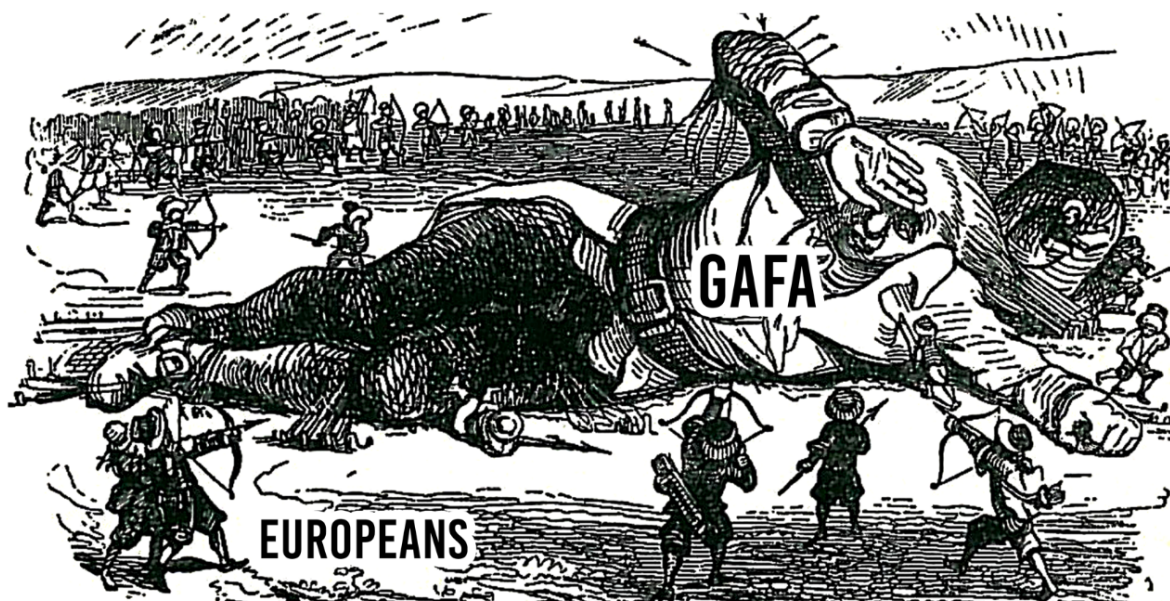
Before detailing EU protections and aggression against U.S. firms and workers, it's worth looking at two issues: Brexit and digital sovereignty. When the United Kingdom was deciding whether to leave the European Union, both Brexit supporters and opponents agreed that leaving the EU would likely mean a decline in EU market opportunities. But what few pointed out was that this was, ipso facto, an indictment of closed EU markets. If EU markets were truly open, as EU officials like to tout, Brexit should not have affected the United Kingdom's trade with the EU. But they are not, and that is why between 2014 and 2020 (Brexit went into effect in 2020), the United Kingdom's trade deficit with the EU was around 26 percent of its exports. By 2023, that had increased to 30 percent.³⁰ Indeed, one study finds that Brexit reduced trade by 20 percent between the EU and Britain.³¹ So much for "free trade" Europe.

The campaign for digital sovereignty is protectionist, pure and simple.

The second issue is the notion of EU digital sovereignty—the claim that leading EU officials make that they should not be dependent on the United States for digital technologies.³² Let's be clear what this means. Imagine if Europe said it wanted steel sovereignty. That would mean no steel imports and no foreign steel makers in Europe. How about wine sovereignty? The same. Thus, the campaign for digital sovereignty is protectionist, pure and simple. And we see a host of

policies and initiatives that Europe is engaging in to achieve its digital protectionism. Perhaps it is time for American luxury car sovereignty.

EU Lilliputians “tying down” the U.S. tech Gulliver



Europe engages in at least three main types of unfair trade activities related to the United States: discriminatory purchasing; revenue extraction and reduced payments; and discriminatory regulations.

Discriminatory Purchasing

In traditional global trade theory, everyone involved—sellers and buyers—is a utility maximizer. If a seller can buy a foreign product that is as good as a domestic one for a lower price, they do. But like so much of neoclassical economics, the reality on the ground is very different from the idealized reality. Europeans generally are not utility maximizers when it comes to trade. National loyalty plays a role, much more than in the United States. And that accrues to their advantage when it comes to trade flows and industry strength.

Consumer Purchases

One factor that limits U.S. exports to the EU is the nationalistic consumption patterns wherein EU consumers exhibit more loyalty to their own country's products. For good or ill, U.S. consumers are largely utility maximizers, having almost no loyalty to domestic companies when it comes to making a purchase. Whatever is cheaper is preferred. Europe is different. Many consumers want to buy national. We see this in the long-standing difficulties in getting to a European single market, especially in services. Policymakers blame the failure on the inability to finish creating streamlined EU-wide regulations, even after more than 30 years of trying. But even if Europe could achieve this regulatory harmonization, Europe would still see services localization because so many EU consumers are nationalistic buyers. Many consumers often won't even buy from European firms outside their country, much less from firms outside Europe.

Take automobiles for example. In Germany, German cars account for around 50 percent of car sales, while French cars account for 5.4 percent.³³ In France, it's the opposite. French vehicles account for 34 percent of sales and German 21 percent. This has nothing to do with transport costs of the autos from the factory and everything to do with consumer nationalism.

European airlines buy Airbus out of EU loyalty, not out of commercial interests.

Commercial Purchases

We see the same pattern in commercial aircraft, where Airbus is unfairly favored in Europe, not only with a history of massive subsidies, but with nationalistic purchasing by EU airline companies. If market forces were the only thing at play, one would expect to see the same share of Airbus purchases in Europe as in other nations. Yet, a sample of three large European airlines (Lufthansa, SAS, and Air France) shows that their fleets are 70 percent Airbus and 13 percent Boeing.³⁴ The top three airlines in America are 39 percent Airbus and 61 percent Boeing. Whereas, in “neutral” countries, four large airlines (Air India, ANA, China Southern, and Singapore) have 43 percent Airbus and 53 percent Boeing. Something other than product value is at work here. European airlines buy Airbus out of EU loyalty, not out of commercial interests, and that not only violates free trade as it is conceived by European policymakers, but it also boosts the EU trade surplus, especially with the United States.

Government Purchases

Consumers and (government influenced or controlled) companies are not the only ones engaged in nationalist buying; so is government. Data from the U.S. Government Accountability Office suggests that the EU uses government procurement to discriminate against U.S. firms. Its report estimates that the EU governments awarded \$300 million to U.S. firms in government procurement in 2015, while the United States awarded \$2.8 billion in procurement awards to EU firms, a level more than nine times higher.³⁵

Extracting Revenue From the United States

A key component of unfair EU trade practices vis-à-vis the United States is a combination of attempts to unfairly extract revenue from American companies and policies to limit the revenue American companies receive from Europe. We see this in many areas.

Digital Service Taxes

Many EU nations have proffered a fanciful notion, which goes against long-standing corporate tax treaties, that foreign (usually U.S.) digital companies should pay corporate taxes to the EU nations rather than to their home country. As the Tax Foundation has written:

Austria, Denmark, France, Hungary, Italy, Poland, Portugal, Spain, Switzerland, Turkey, and the United Kingdom have implemented a DST. Belgium and the Czech Republic have published proposals to enact a DST, and Latvia, Norway, Slovakia, and Slovenia have either officially announced or shown intentions to implement such a tax.³⁶

Digital service taxes are bad policy that provide a thinly disguised effort to target U.S. tech firms. Proponents of DSTs try to justify this tax grab by claiming that users are creating value and therefore that value should be taxed where users reside. (Otherwise, under international

corporate tax agreements, foreign nations would not be allowed to tax other countries' corporate profits.) In fact, users do not create value; companies do. Users consume; digital companies produce.³⁷

Furthermore, taxing profits based on where users reside would violate longstanding international agreements by taxing income more than once and imposing an ad valorem tax that primarily targets imports. DSTs obviously discriminate against a narrow set of highly digital industries, mainly search engines, social media platforms, and online marketplaces. Precisely because they fall mainly on U.S. companies, DSTs also likely violate existing trade agreements, as they act as a prohibited de facto tariff. More specifically, the high revenue thresholds that subject a firm to a DST, and the exclusion of certain revenues widely earned by European firms, create de facto discrimination against U.S. digital firms, in violation of the European Union's national treatment commitment under the General Agreement on Trade in Services.³⁸

Meanwhile, the European Commission also has cracked down on individual member states attempting to attract international investment by offering competitive tax policies. For example, the Commission ruled in 2016 that Ireland wasn't taxing Apple enough and ordered Ireland to collect more than \$14 billion.³⁹ Irish officials defended their tax practices and Apple appealed, but in September 2024 the European Court of Justice ruled in the Commission's favor, ordering Apple to pay Ireland €13 billion (\$14.3 billion) in back taxes.⁴⁰

Exorbitant Fines

At times, it seems as if the Commission is seeking to fund itself by levying exorbitant fines on big American tech companies.⁴¹ For example, in 2017 the European Commission imposed a record-high \$2.3 billion fine on Google for, allegedly, manipulating its search results to favor its own shopping comparison service to the detriment of its rivals.⁴² In contrast, the U.S. Federal Trade Commission found no "search bias" and concluded instead that Google's behavior benefited consumers. In 2018, the European Commission doubled down on Google with an even higher fine of \$5 billion in another competition law case involving Google's operating system Android, followed by a 2019 fine of \$1.7 billion in a case involving Google's AdSense online advertising program.⁴³ In 2024, the Commission levied its third-largest antitrust fine ever: \$1.9 billion on Apple.⁴⁴ In 2023, the Commission levied a \$418 million fine on chipmaker Intel.⁴⁵ While the United States and EU try to support domestic semiconductor production, including from Intel, the Commission makes it worse. Qualcomm was hit by a \$258 million fine.⁴⁶ While China is trying to build up its tech champions, and tear down American, it turns out that it has an ally in Europe. This does not mean that all fines are unfair, but it's not likely that these finds would be anywhere near as severe if these were EU national champions.

The General Data Protection Regulation (GDPR) is also another important moneymaker for Europe. As of January 27, 2022, of the 900 fines that EU data protection authorities have issued under GDPR, 7 of the top 10 were against U.S. firms, including an \$877 million fine against Amazon and \$255 million fine against WhatsApp.⁴⁷ According to the Information Technology and Innovation Foundation (ITIF) estimates, between 2020 and 2023, EU governments imposed at least \$3.1 billion in fines on U.S. companies under GDPR, equivalent to \$29 per American household.⁴⁸

Network Usage Fees

Because the EU depends heavily on U.S. digital platforms, including content providers, it is seeking yet another way to extract dollars unfairly: in this case, a so-called “fair share” policy for Internet traffic that imposes extra fees on U.S. content companies to subsidize European Internet service providers (ISPs).⁴⁹ This “unfair share” policy would mandate that content providers, such as Netflix and YouTube, pay fees to European ISPs in return for use of the latter’s bandwidth. No other region does this, for the simple reason that broadband customers pay their own ISP to download bits.⁵⁰ Rather than content providers sending data unprompted, it is the ISP’s own customer that is paying to have the data delivered to them. Given this, the “fair” route would be for ISPs worried about too much data use to charge heavy data users more. But going after American content providers is much easier—free money for the EU ISPs and less competition for their own content channels.

Reducing Revenue to the United States

In addition to wanting to extract revenue from U.S. companies, the EU is also seeking to limit revenue going to U.S. companies. We see this in at least two areas: pharmaceuticals and computer hardware and software.

Price Controls on Drugs

Through their draconian price controls, European governments refuse to pay their fair share for U.S.-developed drugs. They free ride off American drug companies’ hard work and massive expenditures to develop new drugs. For example, in 2018, if the Netherlands had paid U.S. prices for drugs, it would have paid 122 percent more, while Germany would have paid 87 percent more and France 84 percent more. These price controls mean a higher U.S. trade deficit with Europe because, by definition, EU consumers are getting imports at a mandatory discount. For example, if Spain, Italy, France, and Germany alone had paid their fair share, the U.S. trade deficit with the EU would have declined in 2018 by approximately \$75 billion.⁵¹ It also means less biopharmaceutical innovation because drug company revenue and research and development (R&D) is less than it would be otherwise.⁵²

Open Source Technologies

The EU pays U.S. companies for hardware and software because these companies have invested billions of dollars to develop intellectual property and high-quality products. The EU doesn’t want to have to pay, so it has long focused on developing open source systems. And let’s be clear: This is about excluding U.S. firms. The EU official open source working group has stated that “the Working Group advocates that this roadmap of activities is supported via coordinated European level actions to avoid fragmentation and ensure that Europe retains technological sovereignty in key sectors.”⁵³ It went on to note, “An open-source ecosystem needs to be stimulated that can act as an alternative to licensing IPs from non-EU third parties.”⁵⁴ This is a euphemism for American companies; in other words, “We don’t want to pay for software imports anymore.”

Discriminatory Regulations

Europe specializes in regulations that discriminate against foreign goods and services, especially American.

Digital Markets Act and Digital Services Act Discrimination

The EU Digital Markets Act (DMA) should have been called the “U.S. Tech Firms Act.” The European Parliament rapporteur for the DMA, Andreas Schwab, suggested that the DMA should unquestionably target only the five biggest U.S. firms (Google, Amazon, Apple, Facebook, and Microsoft).⁵⁵ He stated that the DMA’s revenue threshold (to be designated as a so-called “gatekeeper”) should be 10 billion euros and the market value at least 100 billion.⁵⁶ He went on to say, “Let’s focus on the biggest problems, on the biggest bottlenecks. So, let’s go down the line—one, two, three, four, five—and maybe six with [China]’s Alibaba ... But let’s not start with number seven to include a European gatekeeper to please Biden.”⁵⁷ Basically, the DMA and Digital Services Act (DSA) are designed to cover, almost exclusively, U.S. firms and not their European or Chinese competitors that offer similar services.⁵⁸ A leaked draft of the proposed EU DSA is quite clear on the intent: “Asymmetric rules will ensure that smaller emerging competitors are boosted, helping competitiveness, innovation and investment in digital services.”⁵⁹

Essentially, the EU shifting the focus of competition intervention from efficiency to market-structure objectives would push competition law in a new direction toward a structural “big is bad” doctrine. Basically, a company’s size (rather than its conduct) would determine whether the new set of ex ante competition rules apply to it. This approach ignores the dynamic competition that gatekeepers bring to the market, the consumer welfare generated by the existing framework, and the innovation and investment incentives necessary to generate future technological breakthroughs.⁶⁰ The DMA creates the false dichotomy that a digital market can be separated from a nondigital market, rather than seeing it as simply one of many ways for firms to reach consumers (as a business model and distribution mechanism).

Restrictions on Data Flows

Europe, and its courts, has laid down differing (double) standards when scrutinizing U.S. surveillance practices as compared with what it allows for EU member states.⁶¹ Despite this, the United States consistently engages in good faith efforts to work with European counterparts to create new frameworks and special safeguards and mechanisms for redress for European personal data (that don’t even exist for U.S. citizens).

Edward Snowden’s revelations about the U.S. National Security Agency’s intelligence collection programs have led to successive Court of Justice of the European Union (CJEU) cases that have restricted and cut off data flows to the United States. CJEU judgments (Schrems I and Schrems II) have invalidated two transatlantic data transfer arrangements: the Safe Harbor Framework and the Privacy Shield Framework.⁶² The United States has definitively discontinued a controversial telecommunications metadata collection program exposed by Snowden.⁶³ It has also enacted other limitations and controls over U.S. surveillance practices.⁶⁴ Ultimately, even the National Security Agency’s revised metadata program hasn’t been reauthorized (it lapsed in 2020), and there are no signs that the Biden administration will try to seek legislative reapproval. The United States is developing new oversight and redress mechanisms as part of negotiations with Europe on a successor agreement to Privacy Shield.

If there is an open question whether data transfers from the EU to the United States comply with new European laws, there is a clear answer on China and other authoritarian regimes: Their safeguards bear no “essential equivalence” to EU standards of privacy.⁶⁵ Never mind the fact the

European Data Protection Board (EDPB) recently conducted a detailed study into government access to data in China, India, and Russia, there are no calls to cut off data to these countries.⁶⁶

At the same time, European governments have received a mostly green light from the CJEU to continue their own bulk metadata programs for national security purposes.⁶⁷ The CJEU opened the door a crack for continued bulk metadata retention for national security purposes in Europe in the recent “La Quadrature du Net and Others” judgment.⁶⁸ (European policymakers have long deflected calls of hypocrisy, as Article 4(2) of the Treaty of European Union states that “national security remains the sole responsibility of each Member State.”⁶⁹) The CJEU decided that if a member state determines that a “serious threat to national security” exists, it may order service providers to collect and retain bulk metadata, so long as the program is “not systemic in nature.” Soon after, France’s highest administrative court, the Conseil d’Etat, ruled that such a threat existed and that the French government could continue to utilize metadata previously retained for national security purposes.⁷⁰

Meanwhile, Germany has decided to end excessive data retention.⁷¹ At the same time, the EDPB investigated and criticized Europol (the European Union Agency for Law Enforcement Cooperation) after reports showed it had collected a huge amount of personal and sensitive data.⁷² Yet, EU member states and the European Parliament agreed on a new Europol mandate that essentially overruled EDPS’s call for them to delete this data and allowed Europol to continue its data collection practices with new safeguards.⁷³

Import Substitution of U.S. Cloud Services

In 2020, the EU created the GAIA-X project and the European Cloud Initiative, in essence, to replace U.S. cloud providers. As usual, Europe tried to drape its efforts in moral values and seemingly upstanding public policy objectives. Europe framed GAIA-X as an “open, transparent and secure digital ecosystem, where data and services can be made available, collated and shared in an environment of trust.”⁷⁴ It would create European cloud services and a marketplace to exchange data on conditions that apply “European values” to data protection, cybersecurity and data processing.⁷⁵ Yet, from its inception, its true objective—to replace U.S. providers—has been clear. In 2021, Amazon, Microsoft, and Google made up 69 percent of the EU cloud market. Europe’s biggest cloud player, Deutsche Telekom, accounted for only 2 percent.⁷⁶ This isn’t the first time France, Germany, and others have tried to forcibly replace U.S. cloud providers and others, such as search (via the French-supported Qwant search engine, which failed and was bailed out by Huawei in 2021).⁷⁷

GAIA-X is a French-German initiative to help build “tech sovereignty”—to encourage firms to store their data with local alternatives to AWS and other U.S. cloud firms.⁷⁸ GAIA-X is an organization (not an actual cloud provider) that aims to connect different cloud providers and users so data can move freely between them, while abiding by GDPR’s restrictions. Essentially, Europe hopes that it’ll help local firms such as SAP or Deutsche Telekom to become larger and more competitive. In 2019, France’ Finance Minister Bruno Le Maire stated that France had enlisted tech companies Dassault Systemes and OVH to “break the dominance of U.S. companies in cloud computing.”⁷⁹ Indicative of how GAIA-X fits into their plans, in September 2021, France’s digital minister told French GAIA-X participants to “go faster” because they held “in [their] hands ... no more no less than a part of France’s digital sovereignty.”⁸⁰ In October

2021, French President Emmanuel Macron lamented that Europe was “very late” with its sovereign cloud plans.⁸¹

Certain EU nations have passed laws requiring cloud computing services to be physically located in their country. For example, in 2022, France enacted updated “sovereignty requirements” as part of a new cybersecurity certification and labeling program known as SecNumCloud. SecNumCloud’s “sovereignty requirements” disadvantage—and effectively preclude—foreign cloud firms from providing services to government agencies as well as to 600+ firms that operate “vital” and “essential” services.⁸² The latest SecNumCloud guidance (v3.2, March 2022) retains broad data localization requirements for all data (both personal and nonpersonal) and foreign ownership and board limits, which would effectively force foreign firms to set up a local joint venture to be certified under SecNumCloud as “trusted” and thus able to manage European data and digital services. A prior post for the Cross-Border Data Forum also analyzed this proposal and how it breached EU trade law commitments under the World Trade Organization (WTO) Government Procurement Agreement (GPA).⁸³ France is leading efforts to embed SecNumCloud’s “sovereignty” requirements in the European Union Agency for Cybersecurity’s (ENISA’s) Cybersecurity Cloud Services scheme, which is under development.⁸⁴

The latest version of SecNumCloud explicitly requires suppliers of cloud computing services to store and process their customers’ data within the EU. This effectively constitutes a ban—or a “zero quota,” in WTO terminology—on the cross-border supply of these services.

Arbitrary Privacy Enforcement

Europe’s selective application of surveillance scrutiny also applies to privacy enforcement. With the death of Privacy Shield, transatlantic data flows face death by a thousand cuts. Privacy activists noyb have filed complaints in all 30 EU and European Economic Area member states against 101 European companies that share data with Google and Facebook.⁸⁵ They plan to file hundreds more.⁸⁶

In January 2022, Austria’s data protection authority found that the use of Google Analytics was a breach of GDPR.⁸⁷ This is the first ruling in this line of complaints, but it’s not going to be the last. In another, separate, case, a Munich court found that a website owner’s use of Google Fonts violated the plaintiff’s “general right of personality” and right of “informational self-determination” of their IP address under §823 of the German Civil Code. Like the Austrian decision, the only personal data submitted to Google was the user’s IP address. Google’s use of standard contractual clauses could not overcome the risk of U.S. government surveillance, no matter how unlikely or unrealistic the scenario that the U.S. government would seek a European user’s IP address based on their specific interaction with an EU-based website’s analytics tooling or font library. It’s privacy fundamentalism given that it essentially means that any IP address shared, for any reason, in any context, with any U.S. entity subject to U.S. surveillance laws likely also exposes personal data.⁸⁸ In February 2022, France’s DPA responded to another noyb complaint and ordered websites to not use Google analytics.⁸⁹

Meanwhile, none of noyb’s complaints were against Chinese, Russian, or other firms using standard contractual clauses to transfer EU personal data. In 2016, Max Schrems stated that firms could use standard contract clauses to transfer EU personal data to China, but not for the United States. Chinese firms could somehow provide assurances that EU personal data could be protected from surveillance in China (where there is no true rule of law and Chinese laws allow

extensive state surveillance).⁹⁰ DPA investigations into Chinese firms, including Mobike (bike share), BGI Group (genetics), and TikTok (social media), remain limited.⁹¹

Standards

Technical standards are key enablers of trade and commerce. The norm is for them to be set by industry-led voluntary bodies. However, the EU has long resisted this process because, like China, it wants to manipulate standards setting to favor its own products and firms.

Now in its bid for “digital sovereignty,” the EU wants to ignore international standards-setting processes (and related trade law) for new technologies such as artificial intelligence (AI). The EU’s theory is that by setting its own standards rather than following standards developed by international organizations, it can promote European “values” in areas such as data protection, cybersecurity, and ethics.⁹² The European Council on Foreign Relations has stated:

If the EU does not set its own standards, it will be forced to adopt standards made by others—who may not share its values. Governance of the internet, including technical governance, is becoming increasingly bifurcated; the danger is that countries will be forced to choose between adopting the standards of a US internet or a Chinese internet, and to thereby give up access to the other market.⁹³

A section written for the Commission is even more clear: “While skepticism remains regarding the readiness and willingness of Member States to harness their strengths collectively towards European technology sovereignty, there is no alternative to do so.”⁹⁴

But the logic and process reek of protectionism. By rejecting global technical standards in favor of its own alternatives, the EU is trying to give its firms an advantage over foreign competitors. For example, the EU’s “common specifications” sound obscure and nonthreatening, but they are potentially powerful tools for protectionism. A common specification is defined as “a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under (laws/regulations).” This requirement features in recent legislation and regulations for medical devices, cybersecurity, the AI Act, machinery products, and the Data Act.⁹⁵ For example, the AI Act specifically mentions it in the context of AI risk management and recordkeeping. In the Data Act, it’s mentioned in relation to building interoperability of common European data spaces. When the Commission creates common specifications for these technologies, it will be mandatory for firms to abide by them to sell into the EU market.

The EU can use common specifications to override or ignore international standards whenever and however it sees fit. For example, it can do so when no harmonized European standard exists or if one needs revisions. It can also do so if one of the three key European standards organizations denies or delays the EU’s request to develop standards; or if the EU simply deems the relevant international standard “unsatisfactory” or does not address European legislative requirements or the EU’s standardization request. The European Commission, at any point over the last few years, could have clarified that common specifications are a tool of last resort and that deference would be given to international standards. Yet, it hasn’t.

The EU could easily engineer a situation to use common specifications, such as setting an unrealistically short deadline for standards or saying they are too slow. For example, the AI Act

sets an unworkable two-year deadline for two European standards bodies to develop a broad and complex set of (local) standards.⁹⁶ Never mind that this task ignores the years of work a joint committee of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) has already done since 2019 on AI standards.⁹⁷ In another case, the Commission released the standardization request for the Accessibility Act to the European Telecommunications Standards Institute (ETSI) at the last possible (legal) moment. It is virtually assured that ETSI will miss the compressed legislative timelines, even though it has already spent years working on relevant standards.⁹⁸

The EU can do this, as common specifications don't have the critical safeguards of standards developed at international organizations—no transparency, inclusiveness, due process, or appeals mechanism. In contrast, the EU can handpick participants—who may not be technology experts but simply Commission officials—to work behind closed doors (away from scrutiny) to develop common specifications that are mandatory in the EU market. WTO members anticipated that countries could try to impose local technical specifications as trade barriers, exactly as the EU is now doing. That's why WTO members have committed to using open, transparent, and voluntary standards.⁹⁹ The EU and its member states are WTO members and are now violating their commitment.

Weaponized Antitrust

Just as China is doing now, Europe has a history of blocking U.S. mergers that pose a competitive challenge to its own firms. Perhaps the most famous of these cases is the blockage of the GE-Honeywell merger in 2001. The EU also blocked a proposed merger with Sun and Oracle, even though U.S. authorities would have allowed it. It's impossible to say with hindsight what would have happened had the EU not blocked these mergers. But Sun went out of business, and it's hard to imagine how General Electric could be any weaker today than it already is. Perhaps if these mergers would have been allowed, Oracle, and especially GE, would be stronger today.

The EU also sought to block the merger of Boeing and McDonnell Douglas, which the EU opposed because it did not want stronger competition to its continental champion Airbus. As Dorothy Robyn, who helped negotiate the deal in the Clinton White House, noted:

The highest drama occurred in 1997, when the EU's chief competition authority, a Belgian-socialist named Karl van Miert, publicly threatened to block the Boeing-McDonnell Douglas merger because of the potential harm to Airbus. (Unlike the United States, with its consumer-focused competition policy, the EU is allowed to consider the impact of a merger on domestic competitors.) A potential trade war was averted when DOD sent a decorated Air Force general to Brussels to explain why the merger was important to the U.S. military.¹⁰⁰

MENU OF OPTIONS

The United States needs to use existing tools better and develop new ones to better target EU protectionism. It needs to be able to “go to the mattresses” and come back with more than a feather duster or toy Nerf gun. The United States does not need to use all its tools at once, but it should start enacting some short-term measures and putting in place the legal and administrative

reforms to create new tools for the future (in case they're needed). In other words, EU policymakers need to know there will be real negative consequences for their continued actions.

At the heart of the United States' approach to European trade should be a focus on the core principles of the multilateral trading system at the WTO: transparency, due process, national treatment, and nondiscrimination. If European laws and regulations don't live up to these core principles—that the EU itself advocates for in supporting the WTO and the global trading system—then it should trigger a ratcheted and targeted response by U.S. policymakers. It's time that the next administration hold the EU up to its own standards, especially in terms of its treatment of U.S. firms.

Doing more than complaining to European officials will likely elicit retaliatory action from Europe. But Europe can't continue to have it both ways: benefiting from cooperation, military assistance, and open trade with the United States while still targeting U.S. firms and trade.

It's time that the next administration hold the EU up to its own standards, especially in terms of its treatment of U.S. firms.

The federal government needs to use both offensive and defensive trade policy measures.

Offensive Trade Policy Options

Amend, and Use, Section 301 to Target Digital Trade Issues

The next Congress should update a main trade defense tool—the Trade Act of 1974—for the digital era by amending it so that it can respond to the type of barriers (digital) that are central to modern trade. Section 301's traditional use of tariffs makes it easy to apply to 20th century trade in goods, but it needs to be amended to create new legal and administrative mechanisms and tools to target service providers. Although Section 301 mentions fees and restrictions on services, it should be amended to detail the mechanism (in terms of responsible agency) and process (in terms of the action, such as licensing, certification, or legal judgment) whereby the administration imposes specific retaliatory measures on a foreign service provider. For example, it should be amended to create a reciprocal joint venture requirement wherein French, German, and Chinese tech and cloud firms would be forced to set up local joint ventures with equivalent ownership and control restrictions that U.S. firms have had to set up in their respective countries.

Pursue a Section 301 Investigation of the DMA and Other Digital Sovereignty Initiatives

The next administration should use Section 301 to initiate an investigation of the DMA, as it is among the most clearly egregious examples of European policymakers targeting U.S. firms. There is a clear case to be made that the DMA would meet the standard for action under section 301 of the Trade Act of 1974. However, an investigation could be broader and include other EU digital sovereignty initiatives, such as discriminatory cybersecurity regulations and exclusively European cloud initiatives. The Biden administration could enact retaliation via tariffs on imported goods (the traditional use of Section 301), taxes or restrictions on EU digital service companies doing business in the United States (a new use of Section 301), and restrictions on other EU service providers, such as accounting firms, air carriers, media companies, automotive companies, aerospace companies, and others.

Use Department of Commerce ICT Service Reviews to Cover EU Firms

The Department of Commerce could interpret new rules regarding the use of information and communications technology (ICT) goods and services by foreign adversaries to apply to transactions with EU firms that use ICT goods and services with those same adversaries. The Rule (86 FR 4909) on Securing the Information and Communications Technology and Services Supply Chain provides a framework for Commerce to unwind ICT services transactions with foreign parties that “(1) involve ICTS [Information and Communications Technology and Services] designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary [defined to include China, Russia, Iran, Cuba, Venezuela, and North Korea]; and (2) poses an undue or unacceptable risk.”¹⁰¹ The rule allows Commerce to review transactions involving a wide range of ICT products and services, including data hosting and computing of sensitive personal data.

Europe is well within the potential scope of application given the Commerce Department’s focus on ensuring that the rule can be used as effectively as possible. Commerce has ruled out categorical exemptions of specific industries or geographic locations, although the secretary of Commerce may consider this possibility in the future. Wholesale exemptions of industries and geographic locations would not serve the rule’s intended purpose of securing the ICTS supply chain because such exemptions would contradict the Commerce Department’s evaluation method for ICTS transactions. Such exemptions would apply to foreign adversaries’ whole classes of ICTS transactions outside the scope of evaluation under this rule.¹⁰²

Impose Mirror Taxes on Countries That Impose Digital Service Taxes

Europe’s (and others’) use of digital service taxes to single out American tech firms for blatantly discriminatory punishment needs a clear response. The Office of the United States Trade Representative (USTR) has already released a detailed Section 301 report on the issue, including the threat of retaliation.¹⁰³ As Gary Hufbauer at the Peterson Institute for International Economics suggests, the United States should amend the Internal Revenue Code to enact a tax on large foreign firms that extracts funds in mirror-image fashion to the discriminatory digital tax on U.S. firms.¹⁰⁴ Section 891 of the Internal Revenue Code (enacted in 1934) provides the legal authority for the president to retaliate against foreign discriminatory or extraterritorial taxes. It allows the president to enact taxes, and to ratchet them up, on foreign citizens and firms. It has never been used. Congress could adapt it for the modern era in mandating a tax on the global revenues of large firms based in France, Italy, and other DST countries when those firms sell goods or services in the U.S. market. The tax could be legislated to expire upon either of two events: agreed international rules that subject tech giants to taxation in countries reached by their platforms or repeal of an individual country’s own DST tax.¹⁰⁵

Create a Cause of Action Allowing U.S. Firms to Sue for DMA-Mandated Disclosure of Trade Secrets and Confidential Information

The DMA specifically targets not only U.S. firms but also core components that make up their competitive and innovation goods and services. The DMA includes a provision requiring “gatekeepers” to disclose certain search engine data (rankings, search data, click and view data) to third-party providers of online search engines upon request and on fair, reasonable, and nondiscriminatory (FRAND) terms. It’s essentially state-directed forced trade secret disclosure (vis-à-vis China’s forced technology transfers).

Congress could create a cause of action in U.S. courts for U.S. firms to obtain financial damages from EU companies that use this provision to obtain their trade secrets and other commercially sensitive information. This would essentially act as a blocking statute to counteract discriminatory EU digital laws and regulations. While the U.S. firms that would potentially use this are small (given the EU is targeting just five firms), it would send a clear signal that there are consequences for unfair and unjustified state intervention into a firm's trade secrets and competitive position.

Limit Transfers of U.S. Citizens' Data to the EU

Thierry Breton, the EU commissioner for internal market, has argued that "European data should be stored and processed in Europe because they belong in Europe. There is nothing protectionist about this."¹⁰⁶ No, actually there is. As such, if the United States and the EU cannot work out an easy-to-administer process by which data can flow seamlessly across the Atlantic, the United States should adopt a similar approach to Europe's: limiting the transfer of U.S.-person data to European companies in Europe.

Defensive Domestic Economic Tools

Limit Federal Procurement Opportunities for EU Firms

The U.S. president has the legal authority to withdraw the Trade Agreements Act waiver for the EU with respect to the Buy American Act program, or for particular categories of EU products/services or suppliers (such as certain technologies or digital services).¹⁰⁷ For example, the president can add or remove end-product categories that are subject to trade agreements in lieu of Buy American Act preferences in Department of Defense (DOD) acquisitions.¹⁰⁸ Similarly, the United States can adjust discretionary preferences under the Foreign Military Sales program. Ultimately, the end result would be similar to how the United States purposely excludes adversaries such as China and Russia from ICT supply chains and procurement (and how U.S. firms and products are excluded from China's and Russia's procurement markets).

Scrutinize Critical Exports to the EU by Removing Their "Favorable" Designation

U.S. policymakers could exclude EU firms from U.S. funds in order to boost U.S. production of medical goods and services. The United States should not be inadvertently bolstering the EU's plan for "strategic autonomy" in the area of medicine to reduce "strategic dependencies" and foster production and investment in Europe. The U.S. Department of Health and Human Services' 100-day supply chain review calls for boosting U.S. production through "a blended mix of targeted investments and financial incentives."¹⁰⁹ Also, to combat the EU's significant trade surplus with respect to pharmaceuticals and incentivize domestic production, the United States could consider imposing tariffs or other import restrictions on EU pharmaceuticals.

Exclude EU Firms From the U.S. Defense Industrial Base

The Biden administration should move ahead with proposed plans (by DOD and Congress) to amend the Defense Production Act to expand the list of countries in which the U.S. government can make industrial investments to produce certain products that support national defense requirements, such as microelectronics and medical supplies. Currently, only the United States and Canada are on the list, but DOD wants to include the United Kingdom and Australia. Until the EU makes clear its commitment to once again embrace Atlanticism, as opposed to fortressing Europe, the administration should ensure that the EU and its member states are not included.¹¹⁰

Retaliate Against Hypocritical Standards for Government Access to Data and Surveillance

The United States should create its own capability to identify and respond to other countries that fail to provide comparable or reasonable safeguards, frameworks, and agreements around government access to data and that otherwise misuse concerns over foreign government access to data to selectively enact restrictions that target U.S. firms. This would support ongoing discussions at the Organization for Economic Cooperation and Development (OECD) on the issue of government access to data. Whether it's national security- or Europol-motivated access to data, EU member states, leaders, and parliamentarians realize that there is a real and legitimate trade-off with privacy at home.¹¹¹ It's time the United States makes sure it recognizes that this also exists internationally, and that selective application of concerns will entail costs. Doing so would ensure foreign countries, especially European ones, could not hypocritically call for changes in the United States that they themselves don't provide at home and only selectively scrutinize certain countries' practices.

The United States, especially after the 2015 passage of the USA Freedom Act (which was the biggest pro-privacy change to U.S. intelligence law since the original enactment of the Foreign Intelligence Surveillance Act in 1978) and other post-Snowden reforms, has been rightfully described by Oxford expert Ian Brown as “the baseline for foreign intelligence standards.”¹¹² Independent analyses, including by the EU's own Fundamental Rights Agency, have documented great variations in rigor among privacy safeguards against surveillance conducted by EU member states under domestic legal authorities.¹¹³

The United States should create an inter-agency body, hosted by Commerce Department, that identifies whether EU member states and other trading partners have similar or equivalent safeguards and oversight for government access to data as the United States does. The Biden administration's Executive Order (EO) on Protecting Americans' Sensitive Data from Foreign Adversaries is relevant, but it mainly targets China's (and Russia's) ability to access U.S. data. But the basis for this EO and its many processes and outcomes are applicable to Europe's selective and hypocritical application of concerns over government access to data.

President Biden's Executive Order number 14034 on “Protecting Americans' Sensitive Data from Foreign Adversaries” provides for cabinet-level assessments and future recommendations to protect against risks from foreign adversaries' access to U.S. persons' sensitive data and involvement in software application supply and development; and also the continuing evaluation of transactions involving connected software applications that threaten U.S. national security.¹¹⁴ It is, in part, based on the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA). The ongoing emergency that President Trump previously declared in Executive Order 13873, “Securing the Information and Communications Technology and Services Supply Chain,” arises from a variety of factors, including the continuing effort of foreign adversaries to steal or otherwise obtain United States persons' data. Biden's EO states that the “continuing effort by foreign adversaries constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States ... To address this threat, the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.”¹¹⁵

The Biden administration should do this via a subsequent, complementary, EO that tasks the secretary of Commerce—in consultation with the secretary of State, secretary of Defense, attorney general, USTR, secretary of Health and Human Services, secretary of Homeland Security, director of National Intelligence, and heads of other agencies as the secretary of Commerce deems appropriate—to work together on the issue. Similar to USTR’s approach to investigating and responding to digital service taxes, the United States should use this investigation into what oversight and safeguards other countries use with regard to privacy and surveillance—and how these compare with the United States’—and identify countries that misuse concerns about privacy, cybersecurity, and surveillance to enact restrictions that target U.S. tech firms and products, while not applying similar scrutiny and restrictions on local and other foreign firms and countries.

In the event the United States finds that countries are unfairly targeting U.S. firms, it could draw up tariffs and other regulatory restrictions to enact against these countries and their own tech firms, but suspend them pending the reasonable conclusion of a U.S.-EU CLOUD Act agreement, negotiations over government access to data at the G7 and OECD, or both.¹¹⁶ Signing up to, and abiding by, a CLOUD Act agreement and potential OECD framework on government access to data would become the basis for ensuring continued market access to the U.S. digital economy given it would represent an international best practice (and genuine, good faith effort on behalf of governments on what is a global issue) on an issue that is often used to disguise digital protectionism.

THE EU AND THE CHINA: BROTHERS IN ARMS?

At first glance, what is remarkable about the list of EU actions against the United States and its tech firms is that it bears a striking resemblance to what China is doing. Both want to weaken the U.S. tech economy so that they can boost their own strength. Both want to displace U.S. tech companies through open source. Both put severe price controls on drugs. Both use antitrust to weaken U.S. firms. Both use government procurement to favor their own firms. Both impose significant fines and other penalties on U.S. firms through antitrust. Both pressure their firms to buy local. Both limit data flows. Both push for open source technologies to become free of American imports. Both use government funding to prop up competitors of U.S. firms. Both pressure U.S. firms to set up data centers there. To be sure, China is much worse in the applications of these tools, but the EU is engaged in similar behavior against the United States.

And both are seeking strategic independence from the United States. The Draghi report states, “These dependencies are often two-way—for example, China relies on the EU to absorb its industrial overcapacity—but other major economies like the US are actively trying to disentangle themselves. If the EU does not act, we risk being vulnerable to coercion.”¹¹⁷ Yes, the United States is trying to disentangle itself from China, an authoritarian state bent on global techno-economic domination. If Europe were astute, it would be doing the same. But the United States is not trying to disentangle itself from the EU. Moreover, the idea that the EU is vulnerable to U.S. coercion is both nonsensical and offensive. Given that the United States has protected Europe with its military, America has had plenty of opportunity to coerce the EU and never has.

BUT WAIT, ISN'T THE UNITED STATES PROTECTIONIST?

EU officials and experts love to trot out the canard that the United States is protectionist. I have a one-word answer for this question: no. But I will expand it to a six-word answer: \$904 billion U.S. current account deficit.¹¹⁸ To say that the United States is protectionist when it runs the world's largest trade deficit is, frankly, laughable. The EU? It currently runs an account surplus with the rest of the world. Case closed.

But what about Buy America and Buy American provisions that favor U.S. made goods in federal government procurement? Again, a \$904 billion current account deficit with the world, and a \$125 billion goods and services trade deficit with EU. But even if this were not the case, as previously cited, the U.S. government already procures nine times more from the EU than vice versa, so the EU can start complaining about Buy America when that ratio is down to one.

And finally, the big kahuna: the IRA and CHIPS Act subsidies for investing in America in clean energy and semiconductor facilities. First, these kinds of subsidies are par for the course now, being rampant in most Asian nations. Like it or not, the only way to assure domestic production in these kinds of critical industries, especially to compete against the Chinese juggernaut, is to provide investment subsidies. Rather than complain, the EU should wake up and get in the game. And of course, EU firms are eligible for these subsidies. Oh, and let's not ignore that massive launch aid given to Airbus, without which the company would not have survived?¹¹⁹

This all feeds into the popular narrative that “the United States turns its back on the world.”¹²⁰ According to this tale, America was the epitome of global openness and with Trump it became a villain of protectionism, with Europe left to hold aloft the beacon of free trade. It is a reassuring narrative to Europeans, but it is false. First, if the this is true, why is that the U.S. goods and services trade deficit with the European Union as a share of gross domestic product (GDP) actually increased from 0.43 percent in 2016 0.45 percent in 2023?¹²¹ How exactly is that protectionist? Again, if and when the EU runs a trade deficit with America, we should talk. Otherwise, stop the posturing.

After criticizing China, Mario Draghi, author of the new report on EU industrial policy, had the audacity to put the United States in the same camp as China, stating, “The US, for its part, is using large-scale industrial policy to attract high-value domestic manufacturing capacity within its borders—including that of European firms—while using protectionism to shut out competitors and deploying its geopolitical power to re-orient and secure supply chains.”¹²²

Mr. Draghi, please explain and give examples of how the Untied States has shut out European competitors from the U.S. market. Moreover, is it using its geopolitical power to re-orient supply chains out of China? Are you really saying that you oppose this? That you trust China and believe that it is playing by the rules and has no designs on becoming the new global hegemon?

Europe is right to focus more on competitiveness, and hopefully the forthcoming Draghi report will include useful recommendations that get implemented. But that strategy should not be one focused on “fortress Europe” against both China and the United States, for not only would that be extremely shortsighted for Europe, but it would also be turning its back on the West and democracy. It is time for Europe to realize that China is the core threat to the West, and that it should be supporting, not attacking, U.S. efforts to limit and protect against the damage from Chinese innovation mercantilism. The goal should be Western competitiveness, not European.

REGAINING ATLANTICISM FOR THE CHINA ERA

Some argue that we must do whatever we can to not alienate the EU so it can help address the China challenge. But that misses the point. As long as the EU views the United States and China as competitors that limit EU technological sovereignty, any efforts by the United States will fail. The EU will not join the fight, preferring to take advantage of the commercial conflict between the United States and China—and it will not roll back its protectionist and mercantilist actions toward the United States.

The United States needs to be clear that the EU must roll these actions back and join with the United States in a new, democratic, free-trade bloc. And if it fails to do so, the United States will respond with countervailing economic force. But if Europe does decide to join with America, then both sides should do whatever they can to strengthen the alliance. This should start with an EU-U.S. trade agreement, which eliminates all tariffs on products traded between the two nations and eliminates virtually all nontariff barriers. This would require EU leadership ignoring the anti-American civil society groups in Europe and both their often nonsensical and antiscientific concerns (such as chlorinated chicken, GMO crops, proposed bans on silicones) and their outright lies about investor-state dispute settlements. The fact that EU interest groups tanked the prior deal is one more bit of evidence of how closed EU markets really are, as well as how unserious the EU is in addressing the critical issues of today's global economy,

Any new, comprehensive trade agreement between the United States and the EU should lay out a cooperative formula for export controls to China, import restrictions on China, commercial counterintelligence sharing vis-à-vis China, and finally, deep advanced technology cooperation, especially in critical industries under threat by China.

CONCLUSION

Since the 1960s, Europe has viewed U.S. IT leadership with alarm. As French economic journalist Jean Jacques Servan-Schreiber wrote in his 1968 bestseller, *The American Challenge*, “One by one, U.S. corporations capture those sectors of the economy most technologically advanced, most adaptable to change, and with the highest growth rates.”¹²³ Like today, Europeans characterized the challenge in dire terms: “a seizure of power,” “invasion,” “domination,” “counterattack,” and “industrial helotry.”¹²⁴

But unlike for today, Servan-Schreiber didn't call for an attack on U.S. firms; he called for Europe to get its house in order: build a single market, fund advanced technology R&D, and expand university enrollment, particularly in STEM (science, technology, engineering, and math). He eschewed any talk of punishing or rejecting U.S. investment. In fact, he wrote, “Nothing would be more absurd than to treat the American investor as ‘guilty’ and to respond by some form of repression.” While the Draghi report does not go as far as Servan-Schreiber did in eschewing anti-American policy, it is far in the right direction.

But to date, EU officials have done little to remedy the EU's problematic and protectionist policies, in part because they know that the transatlantic “blob” (the network of think tanks, influencers, companies, and government officials) committed to a harmonious cross-Atlantic relationship will veto any tough action. It's time to end that, at least in the United States. The next administration should make it clear that unless the EU effectively addresses a significant share of these trade barriers and anti-U.S. policies, the U.S. government will take firm action.

And the faster that the EU can recognize that the challenger is not America but rather China, the sooner we can get on with forging a much more productive relationship. However, should the EU continue to choose to go it alone, seeing the United States and China each as threats, it will lose. Its only hope is a strong alliance with the United States, and that will not happen as long as the EU continues to discriminate against U.S. companies.

Finally, if the United States makes it clear that it will no longer accept this kind of discriminatory EU behavior, the EU hopefully will realize that it has to modify its approach. Then and only then can we reestablish a strong Atlanticism for the 21st century—one based on much deeper cooperation, including in advanced technology—in order to not succumb to the Chinese advanced technology challenge. The idea that the EU can be competitive in advanced industries on its own, and against both China and the United States, is ludicrous. China, not the United States, is the threat to Europe. This is equivalent to Europe saying in the height of the Cold War that it wanted to be unaligned and compete militarily and economically with both the Soviet Union and the United States.

Acknowledgments

The author wishes to thank ITIF's former associate director of trade policy, Nigel Cory, for providing input to this report. The author also thanks to Meghan Ostertag for her help with data collection and analysis. Any errors or omissions are the author's responsibility alone.

About the Author

Dr. Robert D. Atkinson (@RobAtkinsonITIF) is the founder and president of ITIF. His books include *Technology Fears and Scapegoats: 40 Myths About Privacy, Jobs, AI and Today's Innovation Economy* (Palgrave MacMillian, 2024), *Big Is Beautiful: Debunking the Myth of Small Business* (MIT, 2018), *Innovation Economics: The Race for Global Advantage* (Yale, 2012), *Supply-Side Follies: Why Conservative Economics Fails, Liberal Economics Falts, and Innovation Economics Is the Answer* (Rowman Littlefield, 2007), and *The Past and Future of America's Economy: Long Waves of Innovation That Power Cycles of Growth* (Edward Elgar, 2005). He holds a Ph.D. in city and regional planning from the University of North Carolina, Chapel Hill.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. Scott Lavery, “Rebuilding the Fortress? Europe in a Changing World Economy” (Review of International Political Economy, 2023), 330–53.
<https://www.tandfonline.com/doi/full/10.1080/09692290.2023.2211281#abstract>.
2. Mary Lovely and Jing Yan “While the US and China decouple, the EU and China deepen trade dependencies” (Peterson Institute for International Economics, August 2024),
<https://www.piie.com/blogs/realtime-economics/2024/while-us-and-china-decouple-eu-and-china-deepen-trade-dependencies>.
3. President Kennedy linked the continued presence of American troops in Europe to a resolution of U.S. payments difficulties, stating, “Europeans must be prevented] from actions which make our balance of payments worse ...The question of the American balance of payments constituted one of greatest concerns ...The threat of withdrawing our troops is about the only sanction we have.” Francis Gavin, “The Gold Battles within the Cold War: American Monetary Policy and the Defense of Europe, 1960–1963” (Diplomatic History, Volume 26, Issue 1, January 2002, Pages 61–94),
<https://academic.oup.com/dh/article-abstract/26/1/61/394028>.
4. Sebastian Lumet and Sabine Weyand, “The Double Integration Doctrine, a Conversation With Sabine Weyand,” group d’études géopolitique, January 2022, <https://geopolitique.eu/en/2022/01/31/the-double-integration-doctrine-sabine-weyand/>.
5. European Commission president Ursula von der Leyen clearly stated regarding the EU’s protectionist’s objectives, “We must have mastery and ownership of key technologies in Europe,” naming quantum computing, AI, blockchain, and critical chip technologies as examples. “Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme,” November 2019,
https://ec.europa.eu/commission/presscorner/detail/es/speech_19_6408.
6. Matthias Bauer and Fredrik Erixon, “Europe’s Quest for Technology Sovereignty: Opportunities and Pitfalls” (European Centre for International Political Economy, May 2020),
<https://ecipe.org/publications/europes-technology-sovereignty/>.
7. “Angela Merkel urges EU to seize control of data from US tech titans,” *Financial Times*, November 2019, <https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca>; “France pledges billions in fight to stop French start-ups heading to United States,” *The Local*, September 2019,
<https://www.thelocal.fr/20190919/france-makes-major-investment-in-homegrown-start-ups/>.
8. For example, for several EU member states, strategic autonomy often means avoiding dependence on European economic and political powers.
9. “Germany calls on EU to tighten grip on Big Tech,” *Financial Times*, November 2019,
<https://www.ft.com/content/2d538f22-048d-11ea-a984-fbbacad9e7dd>.
10. Radio Classique (@radioclassique) “#Gafa : @BrunoLeMaire a accusé les géants du numérique d’être les ‘adversaires des états.’ Retrouvez l’Invité politique de @guillaume_durand du lundi au jeudi à h15 sur @radioclassique” (November 2020),
<https://twitter.com/radioclassique/status/1324006008235134978>.
11. “European Commission (2020a), Communication from the Commission: A New Industrial Strategy for Europe,” March 2020, https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf; “European Commission (2020b), Communication from the Commission: Shaping Europe’s digital future,” February 2020,
https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf; “European Commission (2020c), Communication from the Commission: A European strategy for data,” 1February 2020,
https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

12. “Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme” (European Commission, November 2019), https://ec.europa.eu/commission/presscorner/detail/es/speech_19_6408.
13. “The Double Integration Doctrine, a Conversation With Sabine Weyand,” group d’études géopolitique, <https://geopolitique.eu/en/2022/01/31/the-double-integration-doctrine-sabine-weyand/>.
14. Ibid.
15. Ibid.
16. Ibid; “Trade Policy Review EN An Open, Sustainable and Assertive Trade Policy” (European Commission, February 2021), https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf.
17. “The future of European competitiveness: Part A, A competitiveness strategy for Europe” (European Commission, September 2024), 30, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en.
18. In the 1960s, France was the first European country to denounce a technological gap between Western Europe and the United States. This coincided with the formation of the OECD, which started work on the promotion and comparative analysis of national science policies. P. Cognard, 1964, “Recherche scientifique et indépendance,” *Le Progres scientifique*, 76, September 1964; Benoit Godin, “Technological Gaps: Quantitative Evidence and Qualitative Arguments” (Project on the History and Sociology of S&T Statistics, Working Paper No. 23, 2003), http://www.csiic.ca/PDF/Godin_23.pdf.
19. “Foreign Relations of the United States 1964-1968,” Volume 34, <https://history.state.gov/historicaldocuments/frus1964-68v34>.
20. “Report of the Interdepartmental Committee on the Technological Gap, Memorandum From the President’s Special Assistant for Science and Technology (Hornig) to President Johnson,” December 22, 1967, <https://history.state.gov/historicaldocuments/frus1964-68v34/d11>; Benoit Godin, “Technological Gaps: Quantitative Evidence and Qualitative Arguments (Project on the History and Sociology of S&T Statistics,” Working Paper No. 23, 2003, http://www.csiic.ca/PDF/Godin_23.pdf.
21. “The future of European competitiveness: Part A, A competitiveness strategy for Europe” (European Commission, September 2024), https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en, p. 01
22. Eurostat, “USA-EU – International Trade in Goods Statistics,” accessed October 2024, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics#Trade_with_the_United_States_by_EU_Member_State.
23. U.S. Census Bureau, “U.S. Trade in Goods by Country,” accessed September 2024, <https://www.census.gov/foreign-trade/balance/index.html>.
24. Eurostat, “International trade in goods – detailed data: EU trade since 1999 by SITC,” accessed September 2024, https://ec.europa.eu/eurostat/databrowser/view/ds-018995_custom_13050014/settings_1/table?lang=en.
25. U.S. Census Bureau, “Exports and Imports by NAICS Commodities,” accessed September 2024, <https://usatrade.census.gov/data/Perspective60/View/dispsview.aspx>.
26. Ibid.
27. IMF categorizes services trade data into nine broad categories in the balance of payments accounts. Telecommunications, computer, and information services are defined as “Telecommunications services include the broadcast or transmission of sound, images, data, or other information by electronic means. These services do not include the value of the information transmitted. Computer services consist of hardware- and software-related services and data processing services. Sales of customized software and related use licenses, as well as licenses to use noncustomized software with

- <https://apnews.com/article/apple-european-union-tech-b1575db8c8c03e5ac8dcd32f94f7984f>;
Shane Tews, “Apple’s Tax Triumph Turned Sour: Is the EU Playing Fair?” American Enterprise Institute, September 17, 2024, <https://www.aei.org/technology-and-innovation/apples-tax-triumph-turned-sour-is-the-eu-playing-fair/>.
41. Anu Bradford et al., “The Global Dominance of European Competition Law Over The Global Dominance of European Competition Law Over American Antitrust Law,” *Journal Of Empirical Legal Studies*, Vol. 16, P. 731, 2019, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3517&context=faculty_scholarship.
 42. “Summary of Commission decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement,” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XC0112%2801%29>.
 43. The European Commission Press Release of July 18, 2018, http://europa.eu/rapid/press-release_IP-184581_en.htm; European Commission Press Release IP/19/1770, “Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising” (March 20, 2019), http://europa.eu/rapid/press-release_IP-19-1770_en.htm.
 44. Agence France Presse, “EU’s Five Biggest Antitrust Fines On Big Tech,” *Barron’s*, March 2024, <https://www.barrons.com/news/eu-s-five-biggest-antitrust-fines-on-big-tech-62979fed>.
 45. Ibid.
 46. Foo Yun Chee, “Qualcomm looks to Europe court again to overturn antitrust fine,” *Reuters*, March 2023, <https://www.reuters.com/technology/qualcomm-looks-europe-court-again-overturn-antitrust-fine-2023-03-13/>.
 47. “30 Biggest GDPR Fines So Far (2020, 2021, 2022)” (Tessian, May 2022), <https://www.tessian.com/blog/biggest-gdpr-fines-2020/>; <https://www.privacyaffairs.com/gdpr-fines/>.
 48. Masha Komnenic, “61 Biggest GDPR Fines & Penalties So Far [2024 Update]” (Termly, February 2024), <https://termly.io/resources/articles/biggest-gdpr-fines/>; <https://www.enzuzo.com/blog/biggest-gdpr-fines>.
 49. Jessica Dine and Joe Kane, “Feedback to the European Commission on the Future of the Electronic Communications Sector and Its Infrastructure: Fair Contribution by All Digital Players” (ITIF, May 2023), <https://itif.org/publications/2023/05/18/feedback-to-european-commission-on-future-of-electronic-communications-sector/>.
 50. Ibid.
 51. Trelysa Long and Stephen Ezell, “The Hidden Toll of Drug Price Controls: Fewer New Treatments and Higher Medical Costs for the World” (ITIF, July 2023), <https://itif.org/publications/2023/07/17/hidden-toll-of-drug-price-controls-fewer-new-treatments-higher-medical-costs-for-world/>.
 52. Stephen Ezell and Kelli Zhao, “How Skeptics Misconstrue the Link Between Drug Prices and Innovation” (ITIF, September 2023), <https://itif.org/publications/2023/09/05/how-skeptics-misconstrue-the-link-between-drug-prices-and-innovation/>.
 53. “Recommendations and roadmap for European sovereignty on open source hardware, software and RISC-V Technologies” (European Commission, September 2022), <https://digital-strategy.ec.europa.eu/en/library/recommendations-and-roadmap-european-sovereignty-open-source-hardware-software-and-risc-v>.
 54. Ibid.
 55. Foo Yun Chee, “EU tech rules should only target dominant companies, EU lawmaker says,” *Reuters*, June 2021, <https://www.reuters.com/technology/eu-tech-rules-should-only-target-dominant-companies-eu-lawmaker-says-2021-06-01/>.

56. Ibid.
57. Javier Espinoza and James Politi, “US warns EU against anti-American tech policy” (ARS Technica, June 2021), <https://arstechnica.com/tech-policy/2021/06/us-warns-eu-against-anti-american-tech-policy>.
58. “The Implications Of The DMA For External Trade And Eu Firms” (June 2021), 21–35, <https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/8/568/1623318729/copenhagen-economics-study-of-dma-implications-on-eu-external-trade.pdf>.
59. “Brussels looks to impose two-tier Big Tech regulation,” *Financial Times*, December 2020, <https://www.ft.com/content/bb681171-3673-46e5-a243-9c18d97e22d5>.
60. Meredith Broadbent, “Implications of the Digital Markets Act for Transatlantic Cooperation” (CSIS, September 2021), <https://www.csis.org/analysis/implications-digital-markets-act-transatlantic-cooperation>.
61. Kenneth Propp, “U.S. and European Surveillance Law Regimes: Time to Adjust the Contrast?” (Cross Border Data Forum, June 2021), <https://www.crossborderdataforum.org/u-s-and-european-surveillance-law-regimes-time-to-adjust-the-contrast/>.
62. The High Court Commercial, “The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems” (2016 No. 4809), https://iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf; “Judgement of the Court” (July 2016), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=12284425>.
63. Robert Chesney, “Three FISA Authorities Sunset in December: Here’s What You Need to Know,” *Lawfare*, January 2016, <https://www.lawfareblog.com/three-fisa-authorities-sunset-december-heres-what-you-need-know>.
64. “US Surveillance Law, Safe Harbor, and Reforms Since 2013: Peter Swire” (December 2015), <http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf>.
65. Kenneth Propp and Peter Swire, “Geopolitical Implications of the European Court’s Schrems II Decision,” *Lawfare*, July 2020, <https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>.
66. “Legal study on Government access to data in third countries” (European Data Protection Board, November 2021), https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en.
67. Kenneth Propp, “U.S. and European Surveillance Law Regimes: Time to Adjust the Contrast?” <https://www.crossborderdataforum.org/u-s-and-european-surveillance-law-regimes-time-to-adjust-the-contrast/>.
68. “Judgment of the Court, October 2020,” InfoCuria, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6447860>.
69. Consolidated version of the Treaty on European Union - TITLE I COMMON PROVISIONS - Article 4, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M004>.
70. “French Council of State discovers the ‘philosopher’s stone’ of data retention” (About intel, April 2021), <https://aboutintel.eu/france-council-of-state-ruling/>.
71. Bundesministerium der Justiz (@bmj_bund), “‘We will put an end to the current practice of data retention as permitted by German law, as we consider it to be a disproportionate encroachment on fundamental rights.’ @MarcoBuschmann, Federal Minister of Justice, Keynote #GermanSymposium, @LSE_GermanSoc” (February 2022), https://twitter.com/bmj_bund/status/1492149172253962240.

72. “EDPS Decision on the own initiative inquiry on Europol’s big data challenge” (European Data Protection Supervisor, October 2020), https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en.
73. Apostolis Fotiadis, “EDPS Decision on the own initiative inquiry on Europol’s big data challenge,” *The Guardian*, January 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_673; <https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data>; Nikolaj Nielsen, “Privacy concerns mount over Europol data collection,” *EU Observer*, February 2022, <https://euobserver.com/democracy/154382>.
74. “The Gaia-X Ecosystem - A Sovereign Data Infrastructure for Europe” (Federal Ministry for Economic Affairs and Climate Action), <https://www.data-infrastructure.eu/GAIA/Navigation/EN/Home/home.html>.
75. Clothilde Goujard and Laurens Cerulus, “Inside Gaia-X: How chaos and infighting are killing Europe’s grand cloud project,” *Politico*, October 2021, <https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/>.
76. “European Cloud Providers Double in Size but Lose Market Share” (Synergy, September 2021), <https://www.srgresearch.com/articles/european-cloud-providers-double-in-size-but-lose-market-share>.
77. Elisa Braun “French search firm Qwant seeks €8M Huawei bailout loan,” *Politico*, June 2021 <https://www.politico.eu/article/french-search-engine-qwant-huawei-bailout-loan>.
78. Janosch Delcker and Melissa Heikkila, “Germany, France launch Gaia-X platform in bid for ‘tech sovereignty,’” *Politico*, June 2020, <https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/>.
79. “France recruits Dassault Systemes, OVH for alternative to U.S. cloud firms,” *Reuters*, October 2019, <https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1W1189>.
80. “Inside Gaia-X: How chaos and infighting are killing Europe’s grand cloud project,” *Politico*, <https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/>.
81. “Cloud souverain: Emmanuel Macron admet des ‘retards’ mais poursuit les investissements” (BFM Business, October 2021), https://www.bfmtv.com/economie/entreprises/industries/cloud-souverain-emmanuel-macron-admet-des-retards-mais-poursuit-les-investissements_AN-202110120257.html.
82. Nigel Cory, “France’s ‘Sovereignty Requirements’ for Cybersecurity Services Violate WTO Trade Law and Undermine Transatlantic Digital Trade and Cybersecurity Cooperation” (ITIF, May 2022), <https://itif.org/publications/2022/05/10/france-sovereignty-requirements-cybersecurity-services-violate-wto-trade/>.
83. Ibid.
84. Ibid.
85. Data Transfers, “101 Complaints on EU-US transfers filed” (noyb, August 2020), <https://noyb.eu/en/101-complaints-eu-us-transfers-filed>.
86. Linda Thompson, “It’s ‘None of Your Business’: The Privacy Nonprofit Founded by Lawyer Max Schrems Is Gearing Up” (ALM, December 2021), <https://www.law.com/international-edition/2021/12/08/its-none-of-your-business-the-privacy-nonprofit-founded-by-lawyer-max-schrems-is-gearing-up/>.
87. Matt Burgess, “Europe’s Move Against Google Analytics Is Just the Beginning,” *Wired*, January 2022, <https://www.wired.co.uk/article/google-analytics-europe-austria-privacy-shield>.
88. Carey Lening, “Regulators are Playing a Dangerous Game on the Internet” (GRC World forums, February 2022), <https://www.grcworldforums.com/legal-and-regulation/regulators-are-playing-a-dangerous-game-on-the-internet/4040.article>.

89. “Transferts de données vers les États-Unis: la Commission européenne adopte une nouvelle décision d’adéquation” (CNIL, July 2023), <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>.
90. Peter Swire (@peterswire) “Max #Schrems, please listen to 1:10 to 1:12 on the recording. you were speaking about using standard contractual clauses to China, and said one would ‘have to look at specific companies and specific safeguards.’ What safeguards could work from China for #surveillance?” (Twitter, July 2020), <https://twitter.com/peterswire/status/1287551706150998016>; <https://soundcloud.com/justin-hemmings-44462987/privacy-in-the-eu-and-us-a-debate-between-max-schrems-and-peter-swire>; <https://www.euractiv.com/section/digital/opinion/in-protecting-europes-data-can-eu-regulation-keep-up-with-chinese-tech/>.
91. “Mobike faces probe by Berlin data protection regulator,” *Financial Times*, November 2022, <https://www.ft.com/content/4c180f4e-fa2c-11e8-af46-2022a0b02a6c>; “German state DPA investigates potential link to malign Chinese genetics firm” (IAPP July 2021), <https://iapp.org/news/a/german-state-dpa-investigates-potential-link-to-malign-chinese-genetics-firm/>; Natasha Lomas, “Ireland probes TikTok’s handling of kids’ data and transfers to China,” *Tech Crunch*, September 2021, <https://techcrunch.com/2021/09/15/ireland-probes-tiktoks-handling-of-kids-data-and-transfers-to-china/>.
92. Tambiama Madiega, “Digital sovereignty for Europe” (Briefing, EPRS Ideas Paper, July 2020), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).
93. Ulrike Franke and Jose Torreblanca, “Geo-tech politics: Why technology shapes European power” (European council on Foreign Relations, July 2021), <https://ecfr.eu/publication/geo-tech-politics-why-technology-shapes-european-power/>.
94. Jacob Elder, “Technology Sovereignty Of The EU: Needs, Concepts, Pitfalls And Ways Forward” (European Commission, 2024), https://ec.europa.eu/assets/rtd/srip/2024/ec_rtd_srip-report-2024-chap-08.pdf.
95. “In vitro diagnostic medical devices - common specifications: About this initiative” (European Commission, March 2022), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13304-In-vitro-diagnostic-medical-devices-common-specifications_en; “Regulation Of The European Parliament And Of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020” (European Commission, September 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454>; Proposal for a Regulation Of The European Parliament And Of The Council: Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts” (European Commission, April 2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>; “Revision of the Machinery Directive (REFIT) In “A Europe Fit for the Digital Age” (Legislative Train Schedule: European Parliament, September 2024), <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-revision-of-the-machinery-directive>; “Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)” (European Commission, February 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068>.
96. Nigel Cory and Patrick Grady, “The EU’s Approach to AI Standards Is Protectionist and Will Undermine Its AI Ambitions” (Center for Data Innovation, February 2023), <https://datainnovation.org/2023/02/the-eus-approach-to-ai-standards-is-protectionist-and-will-undermine-its-ai-ambitions/>.
97. “Information technology – Artificial intelligence – Artificial intelligence concepts and terminology” (AI Standards Hub, July 2024), <https://aistandardshub.org/ai-standards/information-technology-artificial-intelligence-artificial-intelligence-concepts-and-terminology/>.

98. “Accessibility requirements for ICT products and services” (ETSI: Harmonized European Standard, March 2021), https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.
99. “Technical Barriers to Trade” (World Trade Organization), https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm#:~:text=The%20Technical%20Barriers%20to%20Trade,create%20unnecessary%20obstacles%20to%20trade.
100. Dorothy Robyn “Lina Khan’s Defective Critique of Boeing as ‘National Champion’” (ITIF, March 2024), <https://itif.org/publications/2024/03/27/lina-khans-defective-critique-of-boeing-as-national-champion/>.
101. “86 FR 4909 - Securing the Information and Communications Technology and Services Supply Chain” (GovInfo, January 2021), <https://www.govinfo.gov/app/details/FR-2021-01-19/2021-01234/summary>.
102. Ibid.
103. “Report on France’s Digital Services Tax Prepared in the Investigation under Section 301 of the Trade Act of 1974” (Office of the United States Trade Representative Ambassador Robert E. Lighthizer, December 2019), https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdf.
104. Gary Hufbauer, “How Congress Can Help Overturn the French Digital Tax” (PIIE, January 2020), <https://www.piie.com/blogs/realtime-economic-issues-watch/how-congress-can-help-overturn-french-digital-tax>.
105. Ibid.
106. Vincent Manancourt and Melissa Heikkila, “EU eyes tighter grip on data in ‘tech sovereignty’ push,” *Politico*, October 2020, <https://www.politico.eu/article/in-small-steps-europe-looks-to-tighten-grip-on-data/>.
107. 19 U.S.C. § 2511(c) authorizes the President to “modify or withdraw any waiver ... or designation” granted pursuant to the TAA.
108. Defense Production Act of 1950, as amended, Section 721(f)(5), [https://investmentpolicy.unctad.org/investment-laws/laws/218/united-states-of-america-section-721-of-the-defense-production-act-of-1950#:~:text=\(5\)%20Clarification.,its%20application%20to%20critical%20infrastructure](https://investmentpolicy.unctad.org/investment-laws/laws/218/united-states-of-america-section-721-of-the-defense-production-act-of-1950#:~:text=(5)%20Clarification.,its%20application%20to%20critical%20infrastructure).
109. Biden Administration 100-Day Supply Chain Review Report at 209, <https://aspr.hhs.gov/ibx/Pages/supply-chain-100-days.aspx>.
110. Justin Doubleday, “Pentagon eyes allied Defense Production Act expansion to shore up critical supply chains” (Federal News Network, September 2021), <https://federalnewsnetwork.com/defense-main/2021/09/pentagon-eyes-allied-defense-production-act-expansion-to-shore-up-critical-supply-chains/>.
111. Mark Scott and Vincent Manancourt, “Europe to US: Pass new laws if you want a data-transfer deal,” *Politico*, June 2021, <https://www.politico.eu/article/europe-to-us-pass-new-laws-if-you-want-data-transfer-deal-privacy-regulation/>.
112. “Geopolitical Implications of the European Court’s Schrems II Decision,” *Lawfare*, July 2020, <https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>; “USA Freedom Act is Biggest Intel Reform in 40 Years” (IAPP), <https://iapp.org/news/a/swire-usa-freedom-act-is-biggest-intel-reform-in-40-years/>.
113. “Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update” (European Union Agency for Fundamental Rights,

- October 2017), <https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu>.
114. Executive Order 14034, “Protecting Americans’ Sensitive Data From Foreign Adversaries,” June 9, 2021, <https://www.govinfo.gov/content/pkg/FR-2021-06-11/pdf/2021-12506.pdf>.
115. Ibid.
116. “CLOUD Act Resources” (Criminal Division), <https://www.justice.gov/dag/cloudact>.
117. “The future of European competitiveness,” European Commission, September 2024, 3, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en.
118. “International Data: International Transactions, International Services, and International Investment Position Tables” (Bureau of Economic Analysis, September 2024), https://apps.bea.gov/iTable/?ReqID=62&step=2&_gl=1*c8gqe1*_ga*MzQ3MDIzMjAzLjE3MTk5MjkxMzA.*_ga_J4698JNNFT*MTcyNDc5MTYxOC40LjEuMTcyNDc5MTY1MC4yOC4wLjA.#eyJhcHBpZCI6NjlsInNOZXBzIjpbMiw2XSwiZGFOYSI6W1siVGFiVGVMaXN0IiwMSJdXX0=.
119. Robyn, “Lina Khan’s Defective Critique of Boeing as ‘National Champion.’”
120. Antonina Bakardjieva Engelbrekt et al., *The Borders of the European Union in a Conflictual World* (Palgrave Macmillan, 2024), <https://library.oapen.org/bitstream/handle/20.500.12657/90425/978-3-031-54200-8.pdf?sequence=1#page=59>.
121. ITIF analysis of IMF, “Current account balance, percent of GDP,” accessed August 28, 2024, https://www.imf.org/external/datamapper/BCA_NGDPD@WEO/?year=2022.
122. Mario Draghi, “Mario Draghi: Radical Change—Is What Is Needed,” group d’études géopolitique, April 2024, https://geopolitique.eu/en/2024/04/16/radical-change-is-what-is-needed/?trk=feed-detail_main-feed-card_reshare_feed-article-content%5bii.
123. Jean Jacques Servan-Schreiber, *The American Challenge*, 1968, <https://www.amazon.com/American-Challenge-Jean-Jacques-Servan-Schreiber/dp/0689102461>.
124. Ibid.