ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of:

Robert D. Atkinson
President
Information Technology and Innovation Foundation

Testimony Before the

U.S. House Ways and Means Committee

Subcommittee on Trade

Hearing on:

Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules

September 20, 2024
Longworth House Office Building, Room 1100
Washington, DC

INTRODUCTION

Chairman Smith, Ranking Member Blumenauer, and members of the Subcommittee. I am Robert Atkinson, President of the Information Technology and Innovation Foundation (ITIF). ITIF has long focused on the intersection between trade policy and digital transformation. Thank you for the opportunity to come before you today to discuss this key issue and what policymakers need to do to ensure the protection of U.S. economic interests.

THE IMPORTANCE OF THE DIGITAL ECONOMY

The digital economy includes firms involved in the entire "stack" of information technology (IT), including chip design, semiconductors, hardware, software, e-commerce, and Internet services. In addition, more and more industries are becoming digital industries relying on computing, communications, and software.

U.S. Internet, software and e-commerce firms are world leaders. Of the top six R&D investors in the world in 2021, five were American tech companies (Amazon, Alphabet, Meta, Microsoft, and Apple), and the other was Huawei. These five firms invested more in R&D than the top 81 Chinese-owned firms combined, with Amazon by itself investing more in R&D than the total amounts invested by Canada, France, or Italy.[1]

In 2022, the gross value added of the digital economy was $2.6 trillion, or 10 percent of U.S. GDP. From 2017 to 2022, while U.S. GDP overall grew at an annual rate of 2.2 percent, the U.S. digital economy grew 7.1 percent per year. The digital economy also accounted for 8.9 million U.S. jobs.

THE GROWTH OF DIGITAL TRADE

The international digital economy has grown two and a half times faster than the global economy over the past 15 years and is now equivalent to over 15 percent of global GDP.[2]

While most think of the digital economy as being driven by large Internet firms, the reality is that many industries are becoming digital. Motor vehicles are "computers on wheels." Manufacturing is "smart." And more. Many "traditional" industries—from oil and gas to manufacturing and retail companies—rely on data from their operations, suppliers, and customers around the world.

THE GROWTH OF "DIGITAL MERCANTILISM"

As the digital economy has grown globally, it has become an increasing focus of policymakers across the world; unfortunately, to often enact unfair and protectionist measures that discriminate against foreign firms. Because U.S. companies lead, these measures have a disproportionate negative impact on U.S. jobs and export earnings. And while it is bad enough that China, is engaged in these practices, unfortunately so too are many U.S. allies.

There are many different types of digital mercantilism practices. But at heart, the lion's share of these policies and practices are discriminatory, designed to either extract money from large American companies, or favor domestic companies and domestic jobs, or both.

Limiting Cross-Border Data Flows

Data localization refers to the practice of countries prohibiting or limiting the transfer of data outside their borders. The number of data-localization measures in force around the world has grown dramatically. In 2017, 35 countries had implemented 67 such barriers. By 2021, 62 countries had imposed 144 restrictions—and dozens more are under

---

1 Trelysa Long and Robert Atkinson, "Innovation Wars: How China Is Gaining on the United States in Corporate R&D," (ITIF, July 2023) https://itif.org/publications/2023/07/24/innovation-wars-how-china-is-gaining-on-the-united-states-in-corporate-rd/.

2 "GTIPA Perspectives: The Importance of E-Commerce, Digital Trade, and Maintaining the WTO E-Commerce Customs Duty Moratorium," (ITIF, October 2020), https://itif.org/publications/2020/10/26/gtipa-perspectives-importance-e-commerce-digital-trade-and-maintaining-wto-e/.

consideration. In 2021, China was the most data-restrictive country in the world, followed by Indonesia, Russia, and South Africa.[3] But many other nations have gotten on the bandwagon. For example, Vietnam's Decree 72 would force foreign firms to store data locally. Firms providing websites (article 37), social networks (article 38), content over mobile telecommunication networks (article 44), and online video games (article 66) would all be forced to store data locally.[4] Bangladesh has gone down the same path.

Nations attempt to justify such practices on privacy and security grounds. But the reality is that nations can have robust domestic rules on privacy and cybersecurity without limiting cross-border data flows. The reason is that national privacy (and cybersecurity) rules follow the data, no matter where it goes. For example, if an American company with a legal presence in a European Union (EU) member state transfers an EU person's data for processing and analysis to the United States, that company does not magically escape the restrictions from Europe's privacy law, the General Data Protection Regulation (GDPR). And if it violates the GDPR either in Europe or the United States, the European national privacy regulator can bring action against the company.

Even if some policymakers will acknowledge that reality, some nations or regions, especially the EU, play the government surveillance card, but often only against the United States. The European Data Protection Board conducted a study into access to data in China, India, and Russia, has not to cut off data to these countries.[5]

Finally, it is important to note that while the free flow of data is important, it is not absolute. Some Internet fundamentalists believe that all data "wants to be free" and there should therefore be no restrictions on data flows, within or between nations. This is like saying just because free trade is good that there should be no barriers to trade in endangered species. When the United States advocates for an open Internet and the free flow of data, it needs to make clear that it is referring to legal data. Child sexual abuse material is clearly not legal, and countries should block such flows. Downloading or streaming digital content without the owner's permission is also illegal and countries should block access to such pirated content.

Government-Driven Import Substitution

Many governments resent U.S. success in digital industries and seek to implement protectionist laws to replace American presence. For example, 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. It's true objective—to replace U.S. providers—is clear. In 2021, Amazon, Microsoft, and Google's cloud services accounted for 69 percent of the EU cloud market. Europe's biggest cloud player, Deutsche Telekom, accounted for only 2 percent.

Cloud Center Localization

Many 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. Its "sovereignty requirements" disadvantage—and effectively preclude—foreign cloud firms from providing services to government agencies as well as to 600-plus firms that operate "vital" and "essential" services. SecNumCloud guidance retains broad data localization requirements for data 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".

---

3 Ibid.

4 Nigel Cory, "How the United States and CPTPP Countries Can Stop Vietnam's Slide Toward China-Like Digital Protection and Authoritarianism," (ITIF, September 2023) https://itif.org/publications/2023/09/08/how-the-united-states-and-cptpp-countries-can-stop-vietnams-slide-toward-china-like-digital-protection-and-authoritarianism/.

5 " 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.

Mandated Edge Provider Payments to Domestic ISPs

A number of nations have proposed or implemented so-called "Fair Share" policies—in which content companies, like streaming services, would be required to pay government-mandated fees to domestic Internet service providers (ISPs) to deliver streaming and other content to consumers. These policies distort the pricing of peering and transit services, disrupting efficient traffic management and raising consumer costs. After adopting such a policy, South Korea has seen higher latency, higher transit and consumer broadband prices, and a decline in available of content.

Similar policies proposed but not yet enacted in Europe and South America suffer from the same fatal flaw of thinking: that there is a free lunch to be had at the expense of American tech companies. By and large, Internet traffic is requested by end users, not arbitrarily sent by content companies. It would be like charging foreign washing machine and refrigerator companies a fee that goes to the local electric utility because these devices use electricity.

Digital Standards Manipulation

Like most technologies, digital technologies are based on standards, ensuring interoperability. These standards process have long been established by a wide variety of voluntary, industry-led standards bodies, which lead to the best standard being adopted.

However, in a bid for its so-called "digital sovereignty," the EU wants to ignore international standards-setting processes (and related trade law) for new technologies such as artificial intelligence (AI). 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 non-threatening, 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. For example, the AI Act specifically mentions it in the context of AI risk management and record keeping. In the Data Act it's mentioned in relation to building interoperability of common European data spaces.

Digital Service Taxes

Many nations have proffered a notion that foreign (usually U.S.) digital companies should pay corporate taxes to their own treasury department rather than to their home country. These are nothing more than raw tax grabs and an array of nations have gone down this road.

All proposals discriminate against large firms. For example, Canada's proposal arbitrarily sets tax thresholds with no logic behind them other than to sweep in the largest U.S. firms.

Proponents of digital services taxes have tried to justify this tax grab by claiming users are creating value and therefore that value should be taxed where users reside. (otherwise under international corporate tax agreements, foreign nations are not allowed to tax other countries' corporate profits.) In fact, users do not create value; companies do. Users consume, digital companies produce. The idea that a Canadian user of Google or Facebook creates value (and hence the service is produced in Canada) is nonsense.

Some, especially in Europe, will argue that that even if value is not created domestically, that these American companies earn revenue in Europe, and therefore should pay corporate taxes there, a tax that would come at the expense of the U.S. Treasury. But if this is case, the United States should impose corporate taxes on all European firms that sell products into the United States, regardless of where their production is located. In other words, a French winemaker who sells their wine to U.S. importer should pay corporate taxes to the United States government. 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.

Aggressive Tech Antitrust

Antitrust enforcement is an easy tool for nations to use to discriminate against foreign firms, in order to boost the relative strength of their own firms. The European Union is the poster child for this. 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. (digital tech) firms (Google, Amazon, Apple, Facebook, and Microsoft).[6] He stated "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."[7]

EU competition law has been weaponized in order to protect European companies and promote competitiveness within the Single Market. This protectionism often happens at the expense of foreign rivals, targeting primarily U.S. tech giants (Alphabet, Amazon, Apple, Meta, and Microsoft), and a Chinese one (ByteDance).

The EU has consistently scrutinized U.S. tech giants for stifling competition. Wrapped in concepts like "ensuring fair competition" and "safeguarding innovation in the digital market," the DMA and the DSA target U.S. Big Tech companies. The so-called "gatekeepers" are defined by revenue and market share thresholds that align with the size of major U.S. tech companies. According to the DMA, gatekeepers must have an annual turnover in the European Economic Area (EEA) of at least €7.5 billion or a market capitalization of at least €75 billion, effectively ensuring that firms like Google, Amazon, Apple, Facebook, and Microsoft are the primary targets. The DSA is designed with similar intentions, stating that "very large online platforms and very large online search engines may cause societal risks, different in scope and impact from those caused by smaller platforms. Providers of such very large online platforms and very large online search engines should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact"

Countries such as Australia, Brazil, India, the United Kingdom, South Korea, and Japan are going down the same road as the EU, without evaluating the copycat DMAs' consequences on consumer welfare and innovation. Moreover, these regulations—similar to the EU's DMA—overwhelmingly negatively affect U.S. firms, while often giving Chinese firms a built-in advantage.

Extractive Fines

Because American technology firms are so large and successful, a number of foreign nations have decided to levy massive fines on them.

Europe is the leading practitioner of this. Indeed, at times it seems as if the Commission is seeking to fund itself by levying exorbitant fines on big American tech companies. For example, in 2017 the European Commission imposed a then record-high $2.3 billion fine on Google, for putting its own shopping comparison service results at the top of the search page. As they say, no consumers were hurt in the making of that decision. This is why the U.S. Federal Trade Commission found no "search bias" and concluded instead that Google's behavior benefited consumers. In 2018, the EU 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.[8] And the EU has brought another antitrust case against Google related to ads. Not counting this case, that would be nearly $9 billion in fines for one company for exclusionary behavior, which for context is 30 percent

---

6 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/.

7 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/.

8 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 2019) http://europa.eu/rapid/press-release_IP-19-1770_en.htm.

more than the fines for more serious cartel behavior that the Department of Justice (DOJ) has gotten over a 10-year period.[9] In 2024, the Commission levied its third largest antitrust fine ever, $1.9 billion on Apple. Just last week the EU's top court validated the Commission's $2.65 billion antitrust fine.

The court upheld a decision that Apple must pay $14.3 billion in back taxes, for supposedly "illegally" receiving tax benefits from Ireland. Apple asserts that the issue is not how much it pays in taxes, but to what government.[10] Moreover, this reeks of hypocrisy from the EU, which restricts state aid to companies, but turns a blind eye to Ireland's undermining of the global tax system with its extremely low corporate tax rate. EC president Margaret Vestager praised the decision as "a big win for European citizens and for tax justice."[11] She could have added "and a big win for EU taxpayers" who now have American companies and consumers paying taxes in Europe.

Moreover, while the United States works to support domestic semiconductor production against Chinese unfair practices and the risk of Chinese invasion of Taiwan, the Commission works to undermine that goal. Qualcomm was hit with a $258 million fine and a $418 million fine on Intel. While China is trying to build up its tech champions, and tear down American ones, it turns out that it has an ally in Brussels.

The GDPR is also another important revenue generator 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 a $877 million fine against Amazon and $255 million fine against WhatsApp. The European Data Protection Board fined Meta $1.3 billion for the audacity of sending data to the United States using a standard contractual clause, something thousands of U.S. companies do. The French privacy regulator fined Google $51 million for not being more transparent on how it used users information to provide targeted ads, even though they present absolutely zero privacy risk (because all that is happening is that a Google computer algorithm matches the information Google already has with an ad that is then shows on the web site). Between 2020 and 2023, EU governments imposed at least $3.1 billion in fines on U.S. companies under the GDPR, equivalent to $29 per American household.[12] For the EU this is an easy decision: their governments get free money while the citizens get free Internet services.

Other nations are seeking large fines on social media companies for content they do not like. Australia is considering legislation that would impose fines up to 5 percent of their global revenue on companies that fail to take down content the government objects to.[13] To put that in perspective, only around 1 percent of X users are in Australia, so in theory it could be fined 5 times the total revenue it receives in Australia.

Taxing Streaming Platforms and Other Tech Companies to Subsidize Domestic Content

A number of countries have decided that they will force U.S. technology companies to pay the government money so it in turn can distribute it to local supplicants: including local news outlets and artists. Case in point, Canada and Australia.

The Canadian Parliament recently passed the Online Streaming Act, which requires foreign streaming services like Netflix, YouTube, and Spotify to extensively promote Canadian content in Canada, and to pay into a fund that supports the creation of Canadian content. The federal government has said that it could see these online streaming services paying over $740 million into a Canadian government media fund, or over 22 percent of the total online streaming market in Canada. These costs will be passed on directly to consumers, with Spotify already doing just that in France

---

9 "Total Criminal Fines & Penalties," https://www.justice.gov/atr/total-criminal-fines.

10 "Apple, Google must pay billions in back taxes and fines, EU court rules," *Washington Post*, September 2024, https://www.washingtonpost.com/world/2024/09/10/apple-google-eu-tax-fine/.

11 Ibid.

12 Masha Komnenic, "61 Biggest GDPR Fines & Penalties So Far [2024 Update]" (Termly, February 2024) https://termly.io/resources/articles/biggest-gdpr-fines/.

13 Byron Kaye, "Australia threatens fines for social media giants enabling misinformation," (Reuters, September 2024) https://www.reuters.com/technology/australia-threatens-fines-social-media-giants-enabling-misinformation-2024-09-12/.

after the French government implemented a streaming tax to support its music sector, even though musicians receive royalties from streaming services.

Similarly, the Australian Arts Commission has issued proposed regulations to tax streaming companies to be used to provide subsidies for Australian artists, even though most if not all of the foreign streaming services host and support Australian content. The idea is that, once again, American companies would pay the government so it in turn can subsidize local artists.

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 have filed complaints in all 30 EU and European Economic Area (EEA) member states against 101 European companies that share data with Google and Facebook. They plan to file hundreds more. Following this, in January 2022, Austria's data protection authority found that the use of Google Analytics is a breach of GDPR.[14] This is 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". Like the Austrian decision, the only personal data submitted to Google was the user's IP address. It's shocking that the German court decided that Google's use of standard contractual clauses (SCCs) were not sufficient to 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. The decision reveals privacy fundamentalism, given 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.[15] In February 2022, France's DPA responded to another complaint and ordered websites to not use Google analytics.

Meanwhile, none of these complaints are 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. That 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) is laughable.

ALLIES ACTIONS

What is striking about these policies is just how widespread they have become, not only among U.S. adversaries and nations that have historically embraced limited free trade, but also among America's core allies.

Canada

While the Canadian-U.S. trade relationship is critical for both nations, it is troubling that Canada is turning to some of the precautionary and protectionist digital trade measures embraced by the EU. Consider some of Canada's major technology policy initiatives over the past year. Many of its efforts have constituted discriminatory policies targeting the tech sector, especially foreign companies. For example, the government has pursued a digital services tax on large technology companies in Canada. Over 140 countries are participating in a multinational process led by the OECD to align corporate tax rules and prevent multinationals from shifting profits to avoid paying taxes. Every country in this group except Canada has agreed to postpone any new digital services taxes for at least another year to give countries time to reach a consensus. In contrast, Canada's Deputy Prime Minister and Minister of Finance Chrystia Freeland has pushed for its 3 percent tax on digital services to go into effect in 2024, a discriminatory measure that would largely

[14] 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.

[15] 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.

impact U.S. technology companies and apply retroactively for the past two years. This proposal would raise prices for Canadian consumers and signal that Canadian policymakers would rather squeeze the tech sector for some fast cash than support its long-term economic growth.

Or consider the Online Streaming Act. The legislation, which received royal assent earlier this year, directs the Canadian Radio-television and Telecommunications Commission (CRTC) to impose domestic content requirements on online streaming services like Netflix, TikTok, and YouTube. These services must now register with the government and pay for and promote Canadian content. Once again, the policy seems more like another cash grab from foreign tech companies rather than a serious attempt at a pro-innovation digital policy that would help Canadian businesses and consumers. After all, if Canadian consumers want to watch Canadian content, these companies have every incentive to provide it to them.

And Canadian lawmakers have not stopped with streaming services. The government also enacted the Online News Act, a law that forces large online news aggregators to pay domestic news publishers for displaying links to their articles. While Canadian news publishers claim they have lost revenue to news aggregators, the reality is that any publisher can easily remove itself from these aggregators, but the overwhelming majority choose not to because it benefits them. Google eventually agreed to pay C$100 million ($73.6 million) annually, indexed to inflation, to a fund for Canadian news publishers. To avoid this shakedown, Meta announced that it would no longer display content and links from news publishers, both Canadian and international, to Canadian users of Facebook and Instagram.

Moreover, in 2021 Quebec adopted a law that limits transfer of personal data to jurisdictions with data protection regimes deemed "adequate." Canada does seem to embrace the free flow of data for pirated content, according to the 2024 USTR Watch list in the Special 301 report.

Korea

Take the case of South Korea, a close ally and hopefully even closer in the fight against Chinese technological dominance. Korea has enacted a range of problematic digital policies that hurt U.S. companies. It blocked access to American ride share companies, including Uber and Lyft. It blocked GPS access to mapping applications for American companies like Google and Apple, even though Korean map application companies have access to it. Its national privacy law includes data localization provisions. Its proposed digital antitrust law (modeled after EU's problematic Digital Markets Act) would discriminate against American firms, while strikingly, exempting most Chinese competitors, and potentially giving Chinese companies access to U.S. company data and technology. Korea has also proposed a tax on American streaming companies with the money to be funneled to Korean ISPs. Its Software Industry Promotion Act restricts bids for government contracts for software services to small and medium sized firms, effectively precluding U.S. multinationals. Likewise, government rules regarding cybersecurity impose restrictive requirements related to government purchases. Its Cloud Security Assurance Program creates significant restrictions for U.S. providers to bid on government cloud contracts. Korea restricts reinsurance firms from moving data outside of Korea, while its financial services regulations impose cloud localization requirements.

WHAT IS THEIR MOTIVATION?

When Willie Sutton was asked why he robbed banks, he said, "because that's where the money is." Foreign countries target U.S. technology firms for the same reason: It's where the money (fines, local revenue, etc.) and jobs are.

However, few countries are as brazen to come out and admit their true motivations. They wrap them in noble sounding goals. Case in point: 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 a central feature.

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 have

explicitly called for both digital protectionism and data sovereignty in talking about digital and technological sovereignty. The French minister for economic affairs went so far as to call U.S. "big tech" companies an "adversary of the state."

While Europe and other developed nations extoll their rationales, many developing nations bring out the old chestnut of resisting colonial exploitation. Many advocates for developing nations have spun a narrative in which data is "the new oil" and cross-border data flows are an extractive, zero-sum process that benefits rich tech firms over impoverished users in low-income nations. Framing it as "data imperialism" leads to demands for change. In this view, users don't get any value from engaging online nor do they have agency to decide what to do online, including whether or not to share their data, or with whom. However, while it is true that the value added to the global economy from data is large, the analogy of colonial extraction is nonsensical. The Internet's ability to connect people, firms, and governments around the world with cloud, search, and other large-scale digital services—at little or no cost to users—is not a plot by the evil "North" to oppress the victims in the "South."

In opposing laws and trade deals that enable data flows and digital trade, critics want countries, especially developing ones, to have "policy space" to enact rules in the "public interest"—both of which are code for protectionist tariff and non-tariff barriers to discriminate against foreign tech firms and support local ones, and/or coercive pressures on tech firms to donate money to local causes.

HOW SHOULD THE UNITED STATES RESPOND?

There is an old saying: "Give them an inch, and they will take a mile." In this case, it might be better put: Give them a kilobit, and they will take a terabit. In other words, because the U.S. government has not made fighting digital mercantilism a top priority—and has even tacitly encouraged it in the last few years—other nations have moved forward with abandon. Why not when you know that there is only an upside. It is time for this to stop and be rolled back. Congress needs to make clear that it expects other nations to cease and desist, while at the same time holding whoever is in the White House to high standards of more strongly incorporating digital issues into a robust trade defense strategy.

Strong Digital Trade Advocacy Does Not Preclude Domestic IT Regulation

One argument we have heard recently for the United States abandoning the field to nations seeking to extract value from the American digital economy is that efforts might contradict domestic policies.

This is what U.S. Trade Representative (USTR) Katherine Tai said to support recent controversial decision to withdraw from key digital trade negotiations at the WTO. The rationale Tai used is that the United States needed to have "policy space" for new laws on privacy and other issues before it can negotiate. She stated that "[USTR would be] committing massive malpractice and probably committing policy suicide by getting out ahead of all of the other conversations and decisions that we need to make as a country." Not only is this not the case, but the opposite is actually true. Given that the United States is the predominant digital economy in the world it is malpractice to not work strenuously to shape the global trading system to maximize digital innovation.

Tai was saying that USTR can't make commitments on data and other digital trade issues until the United States has new laws in place. At one level this makes sense. How can USTR commit the United States to international regulations when domestic ones are not fully fleshed out? In reality, it is clearly not the case that digital trade policy must follow new domestic laws, just as it clearly doesn't apply to any number of U.S. interests and initiatives involving data and new and emerging technologies.

The Biden administration, like every administration before it going back to the Clinton White House, engages internationally on digital issues separate from domestic legislation. For example, the United States doesn't need to pass AI legislation to be able to commit to a trade agreement prohibiting foreign legislation discriminating against foreign firms. The Biden administration's extensive AI executive order shows that the lack of an explicit AI law does not stop it from taking action domestically and internationally. Likewise, the United States doesn't need to pass a national privacy bill (although Congress should) to be able to commit to an agreement prohibiting data localization regimes and other core issues like non-discrimination against foreign firms and digital products.

Moreover, USTR Tai's portrayal of digital trade is simply not borne out in reality. The United States committed to ambitious and legally binding commitments on data flows, data localization, and source code in the USMCA. The USMCA didn't undermine California's Consumer Privacy Act. Nor would it have prevented the proposed American Data Privacy and Protection Act (ADPPA). Neither of these laws contain localization policies or discriminate against U.S. or other foreign firms and their digital products. If the United States enacted the ADPPA, U.S. digital trade law (under USMCA) would already be in alignment, not conflict (as USTR Tai tries to paint it). Not only that, but other Biden administration initiatives like the Global Cross Border Privacy Rules framework would actually support it in providing an additional layer of accountability to ensure that firms protect data when they transfer it overseas.

USTR Tai tries to paint digital trade as if it conflicts with congressional legislative sovereignty and efforts to enact new domestic laws and regulations on privacy, competition policy, content, cybersecurity, and other digital issues. This is clearly not the case. The WTO e-commerce negotiations are led by Australia, Japan, and Singapore, and involve other advanced countries with highly sophisticated regulatory systems, like Canada, Chile, the European Union, Korea, New Zealand, Taiwan, the United Kingdom, and others. These are not labor, human rights, consumer rights, or regulatory scofflaws. Many of these countries have signed several digital trade agreements and these have not stopped them from subsequently enacting new domestic legislation. Digital trade rules, like traditional trade rules, only become a problem when domestic laws and regulations are discriminatory and act as an unnecessary and disproportionate barrier to trade. Herein lies the rub: USTR Tai does not support digital trade as she wants the European Union and other regions/countries to enact discriminatory laws and regulations to target U.S. big tech.

The purpose of U.S. trade policy is to promote trade and investment and protect U.S. interests abroad. Advocating for policies such as the global free flow of data and dissuading other countries from implementing data localization measures directly benefits U.S. trade interests. The United States is a global leader in cloud computing services, and it has the most to lose from restrictive policies that limit the use of U.S.-based data firms. Many countries would gladly implement protectionist measures, like data localization, to disadvantage American tech firms and workers. If USTR is not willing to defend U.S. trade interests abroad, who will?

None of this should be surprising. U.S. global economic, trade, technology, and national security engagement does not depend on the United States having new laws in place for every new issue raised by technology. It's one thing for progressive politicians to push their preferred legislation in Congress, but it's quite another for USTR Tai to dismiss and undermine other parts of the Biden administration and their interests in U.S. global digital and technology policy. USTR Tai's decision shows a concerning disregard for the usual boundaries between domestic debates and support for the U.S. government abroad, given how USTR Tai essentially wants to take U.S. trade policy hostage in the absence of progressive Democrats' preferred competition and antitrust legislation.

USTR's decision helps Beijing advocate for the broad, self-judging exception for national security in trade agreements to justify rules that require data to be stored on local servers. By contrast, Australia, Japan, Singapore, the United Kingdom, and many other U.S. trade partners are negotiating rules so that data flows are the norm and any restrictions to it the exception. For example, members of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (like Australia, Japan, and Singapore) advocate for language at the WTO that protects data flows and ensures that any exceptions to this rule are necessary, not arbitrary, and proportionate. These U.S. allies want WTO negotiations to narrow the scope for domestic "policy space" exceptions to legitimate privacy, cybersecurity, and other policies. While policy space may sound appealing in principle, in practice countries like China have misused this concept in existing WTO agreements, such as on services trade, to enact restrictions that make its trade commitments—whether on data flows, digital goods and services, or other issues—essentially meaningless.

Paradoxically, at the same moment the United States is walking back its stance on free data flows, Beijing has taken significant steps to ease controls over cross-border data transfers. Driven by a slowing economy and declining foreign investment, China's cyber regulator issued a landmark new draft regulation in September that exempts many companies from a mandatory security assessment required to send data out of the country. Beijing is revising long-standing restrictions on data flows, in part, to make the business environment more favorable to businesses, while the United States is sending signals that it intends to do the opposite. That said, implementation of China's policy shift remains

unclear. And even if it were to go into place as written, Beijing could still deem a company's data as linked to national security and, therefore, subject to localization requirements at any moment—consistent with its cyber sovereignty position.

An Indian think tank, the Global Trade Research Initiative, notes that USTR's decision will help ensure that future digital trade agreements provide "policy space" for data sovereignty, stating, "given the US' dominant role in the global digital landscape," this decision "is poised to spark a worldwide reassessment of national e-commerce policies." India's concerns about data sovereignty led it to not join the IPEF's trade pillar and to avoid the WTO e-commerce negotiations. The absence of U.S. advocacy on data flows will inevitably have implications for digital trade policy in other countries in the future.

USTR's decision also undermines U.S. ambitions for global leadership in AI. AI firms in the United States and in other countries depend on access to large, diverse international data sets. If U.S. firms cannot send data out of countries in which they operate overseas, this significantly limits AI researchers and developers who use cross-border data to build applications that work across a variety of geographies, languages, cultures, and demographics. As the technology competition between Washington and Beijing continues to play out less in the United States and China and more in other countries around the world, encouraging trusted data flows among allies and partners is vital to advancing U.S. technological leadership. Although China's large domestic population creates a data advantage, the United States and its partners can offset this by using data flows from around the world, but this relies on continued access to global data sources.

Time to Get Back on the Globalization Horse

To start with, it is time for Congress and the administration to "get back on the globalization horse," and in particular on the digital horse. If the United States is not "in the game" the rules will be set by others in a way that hurts our economy and workers, and America will cede whole parts of the world to Chinese economic predation and European regulatory imperialism.

To be sure, some past trade agreements were too one-sided against the United States. But the reality is that it is China that has caused most of the problem regarding globalization and trade, not trade with most other nations. Rather than abandon trade, which leading figures in each major party now seem to want to do, America needs to reengage, albeit this time in a new way.

First, we need a USTR that seeks to open up more trade, but this time with tougher standards to protect U.S. interests, including, despite what the anti-trade left says, investor-state dispute settlement (ISDS) rules, and what the right says, strong currency manipulation protections. This means signing new trade agreements that are gold-standard agreements when it comes to digital and other agreements, including intellectual property protection.

Second, given the importance of the digital economy, U.S. global IT and digital policy needs to be guided by a grand, overall strategy, focused first and foremost on maintaining U.S. global tech leadership. The United States faces a risk where much of the world, including the EU, could align against U.S. IT and digital interests, leading to a many-against-one environment, with detrimental consequences.

So, to start with in efforts to reestablish closer relations with the EU, the United States should not "give away the store" by allowing the EU to go forward with its increasingly aggressive technology mercantilism. At the same time, the United States must enlist likeminded nations in a variety of ways to support U.S. interests—and it should not be reluctant to exert pressure to encourage these nations to come along.

Domestically, all too often, U.S. thinking about privacy, tech platforms, national security, and Internet and AI governance is siloed and bifurcated. During the Clinton and second Bush administrations, U.S. policymakers believed that the rest of the world would emulate what was obviously the superior U.S. digital policy system, and they worked toward that end. But China's unprecedented success in IT and digital industries, coupled with a questioning of the desirability of a U.S.-style light-touch digital regulation and the rise of U.S. "big tech" companies, has meant that the

United States can no longer rely principally on persuasion to convince others of the economic and innovation advantages of its approach.

Shaping the global IT and digital economy in ways that are in U.S. interests is one of the most important challenges facing U.S. foreign and economic policy going forward. Getting it wrong could lead to a many-against-one environment wherein U.S. IT and digital firms—and by extension, the United States overall—face a challenging environment with consequences for many aspects of American life.

It is long past due to leave behind the hopeful, but naïve, view that most countries will see the digital economy the way the United States has historically seen it: as a force for progress, innovation, and free speech, wherein market outcomes should generally be allowed to prevail, with a light touch of government only in the few places needed. In the future, needed change will come more from appealing to foreign interests, rather than values and ideas.

The U.S. government needs to formulate a grand strategy grounded in a doctrine of digital realpolitik that advances U.S. interests first and foremost, recognizing that it should work with allies when it makes sense, and constrain digital adversaries, especially China and Russia.

It is time for the U.S. government to develop and implement a grand strategy for the global IT and digital economy that is realistic and pragmatic in recognizing how countries enact digital policies and is most likely to appeal to a broad and diverse range of countries—while putting U.S. national interests at the forefront. Failure to do so will risk having the United States surrounded by a host of technology competitors, and in some cases, such as with China and Russia, adversaries, which will lead to diminished U.S. technological, economic, political, and military leadership.

For too long, the United States has either had abstract, ideological strategies such as promoting an open global Internet, or responded piecemeal, fighting each fire as it breaks out. And in both kinds of engagement, it has worked to change hearts and minds by trying to persuade other nations of the superiority of the U.S. system. That might have had some purchase in the 1990s and 2000s when the United States was the early leader in the digital revolution and before the rise of large, global U.S. tech firms. But education and persuasion, while needed, are no longer enough. EU officials, for example, mostly understand the arguments U.S. officials make—they just either don't agree with them or their politics won't allow them to act on them. This is even more true in China, where for years the U.S. approach was to "educate" Chinese officials on the merits of the U.S. system. China didn't need education. They fully knew they were "cheating" and what the United States did not like. It needed pressure and pain.

As such, the U.S. government needs to understand that the major global IT and digital challenges it faces stem not from ignorance, but from ideology and interests. As such, here are four scenarios the U.S. government should work to achieve in the immediate and moderate term.

And while we are at it, Congress should require the USTR to publish a list annually of all the trade barriers and distortions listed in the past National Trade Estimates (NTE) reports which are still in force. It is striking to read the annual USTR NTE and Special 301 reports for the sheer volume of protectionist and other problematic foreign practices affecting trade and U.S. companies. But the real question is how often does the United States prevail in either preventing other nations from implementing proposals, or in the cases of ones already in place, getting nations to roll them back.

Specific Steps to Take

Besides playing the important role of oversight and pressure on the Administration and foreign governments, Congress and the next Administration can and should take some specific steps.

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 judgement) 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. French, German, and Chinese tech and cloud firms would be forced to setup local joint ventures with equivalent ownership and control restrictions that U.S. firms have had to setup in their respective countries.

Pursue a Section 301 Investigation of the DMA (and Other EU 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 whereby European policymakers target 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. If used, 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 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 the Department of Commerce to unwind ICT services transactions with foreign parties that "(1) involve ICTS 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."[16] The rule allows the Department of Commerce to review transactions involving a wide range of ICT products and services, including data hosting and computing of sensitive personal data.

Amend the Internal Revenue Code to Allow Authorities to Impose Mirror Taxes on Countries that Impose Digital Service Taxes

Europe (and other's) use of digital service taxes to single out American tech firms for blatantly discriminatory punishment needs a clear response. USTR has already released a detailed Section 301 Report on the issue, including the threat of retaliation. 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.[17] 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 these up, on foreign citizens and firms. 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 US market.

Congress Could Create a Cause of Action to Allow U.S. firms to Sue for DMA-Mandated Disclosure of Trade Secrets and Confidential Information

The DMA not only specifically targets U.S. firms, but targets 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

---

[16] "86 FR 4909 - Securing the Information and Communications Technology and Services Supply Chain," (GovInfo) https://www.govinfo.gov/app/details/FR-2021-01-19/2021-01234/summary.

[17] Gary Clyde Hufbauer, " How Congress Can Help Overturn the French Digital Tax," (Peterson Institute for International Economics, January 2020), https://www.piie.com/blogs/realtime-economic-issues-watch/how-congress-can-help-overturn-french-digital-tax.

fair, reasonable, and non-discriminatory (FRAND) terms. It's essentially state-directed forced trade secret disclosure (vis a vie 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'd send a clear signal that there are consequences for unfair and unjustified state intervention into a firm's trade secrets and competitive position.

Limit the Transfer of U.S. Citizens' Data to Nations That Limit the Transfer of Their Data

If other nations refuse to allow data flows to the United Sates, then it's time to play hardball. Thierry Breton, the EU commissioner for the internal market, argues that "European data should be stored and processed in Europe because they belong in Europe. There is nothing protectionist about this."[18] 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 of Europe's: limiting the transfer of U.S.-person data to European companies in Europe.

Support the Next Round of Information Technology Agreement (ITA) Expansion

The ITA has been one of the WTO's most successful plurilateral trade agreements. Originally signed in 1996 and to which 82 countries are now signatories, it has eliminated tariffs on trade in hundreds of ICT products through the original agreement and a 2016 expansion which added 200 more products. But digital and information technologies have already evolved considerably since then, and so an initial group of stakeholders has convened to identify over 400 more unique ICT products as candidates for potential ITA inclusion into an "ITA-3." ITIF estimates that if the 82 signatories of the original ITA were to join an expanded ITA-3, the global economy would grow by nearly $766 billion over the ensuing 10 years. Moreover, an ITA-3 expansion could help grow U.S. GDP by $208 billion over a decade, increase U.S. exports of ICT products by $2.8 billion, and help create almost 60,000 U.S. jobs.

Embrace and Extend the Moratorium on Customs Duties on Electronic Transmissions

In 1998, WTO member countries agreed to enact a moratorium on customs duties on electronic transmissions, and have agreed to renew the moratorium roughly every two years, recognizing that the growing global digital economy should be kept duty-free. Some countries have called for ending the moratorium seeking the revenues such duties could bring, but doing so would hurt more than it would help. For instance, one study concludes that developing and least-developed countries would lose more in GDP than they would gain in tariff revenues with the withdrawal of the WTO Moratorium.[19]

Limit U.S. Aid to Countries That Engage in Digital Protectionism

Since the end of WWII, U.S. foreign aid programs have turned a blind eye to foreign mercantilist practices that harmed U.S. techno-economic interests. Now that the United States is no longer in the lead it is not acceptable. When Congress engages in oversight of various federal aid programs, it should investigate and ultimately require that these agencies limit funding that goes to nations that engage in more than de minimus digital mercantilism or IP theft. For example, ITIF has found the U.S. Development Finance Corporation supports many projects in countries on the 301 Watch List and the engage in digital trade restrictions.[20] Equally importantly, U.S. aid and other support, including through

---

[18] 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/.

[19] Hosuk Lee-Makiyama Badri Narayanan Gopalakrishnan, "The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions" (ECIPE, 2019), https://ecipe.org/publications/moratorium/.

[20] Robert Atkinson, " US Development Financing Needs to Stop Rewarding Nations Whose Policies Harm US Companies and Workers," (ITIF, August 2024) https://itif.org/publications/2024/08/12/us-development-financing-stop-rewarding-nations-policies-harm-us-companies/.

organizations such as the World Bank and InterAmerican Development Bank, should be contingent on nations limiting their digital protectionist policies and programs.

Expand State Department and Other Efforts to Educate Developing Nations on the Appropriate Kinds of Digital Regulations and Other Policies

To be sure, some nations embrace digital mercantilism for protectionist means. But often policymakers are not fully aware of the problems with some of their policy proposals, including harm to their digital ecosystem. At the same time, many developing nations need help in crafting pro-innovation digital policies.

Congress needs to increase the budget of the State Department for much stronger digital policy technical assistance to these nations. If all they hear from are EU and Chinese officials, it is unlikely they will adopt the superior U.S. digital policy system. Part of this should include more funding for State and Commerce Department engagement with developing nations, including expanding the digital attachés program, a network of digital trade officers in U.S. embassies currently in 16 markets who help U.S. firms increase their global online market access and navigate regulatory and digital policy challenges. It should also expand the program into new markets in order to continue promoting U.S. firms' global competitiveness.

Congress should press the State Department to lead on a global narrative arguing why the U.S. pro-innovation approach is best for countries. This narrative should include debunking the argument that the EU's "values based" approach is significantly more effective than the U.S. approach at protecting consumers from online harm.

The State Department should push back against the UNCTAD narrative that developing countries are victims of foreign firms, and therefore they are justified to enact protectionist measures, including data localization, to protect their interests in the digital economy.[21] In addition, the State Department should stop funding organizations that misleadingly paint U.S. digital policy and performance in a bad light, including the advocacy group Freedom House's annual Freedom on the Net report, which takes a highly subjective, ideological approach to analyzing Internet freedom.[22]

Thank you for the opportunity to appear before you today on this critical issue of data flows and digital protectionism.

[21] Ash Johnson, "Restoring US Leadership on Digital Policy" (ITIF, July 2023), https://itif.org/publications/2023/07/31/restoring-us-leadership-on-digital-policy/.

[22] Ibid.