

**PROTECTING AMERICAN INNOVATION BY
ESTABLISHING AND ENFORCING STRONG
DIGITAL TRADE RULES**

HEARING
BEFORE THE
SUBCOMMITTEE ON TRADE
OF THE
COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
SECOND SESSION

SEPTEMBER 20, 2024

Serial No. 118-TR06

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2024

57-161

COMMITTEE ON WAYS AND MEANS

JASON SMITH, Missouri, *Chairman*

VERN BUCHANAN, Florida	RICHARD E. NEAL, Massachusetts
ADRIAN SMITH, Nebraska	LLOYD DOGGETT, Texas
MIKE KELLY, Pennsylvania	MIKE THOMPSON, California
DAVID SCHWEIKERT, Arizona	JOHN B. LARSON, Connecticut
DARIN LAHOOD, Illinois	EARL BLUMENAUER, Oregon
BRAD WENSTRUP, Ohio	DANNY DAVIS, Illinois
JODEY ARRINGTON, Texas	LINDA SANCHEZ, California
DREW FERGUSON, Georgia	TERRI SEWELL, Alabama
RON ESTES, Kansas	SUZAN DELBENE, Washington
LLOYD SMUCKER, Pennsylvania	JUDY CHU, California
KEVIN HERN, Oklahoma	GWEN MOORE, Wisconsin
CAROL MILLER, West Virginia	DAN KILDEE, Michigan
GREG MURPHY, North Carolina	DON BEYER, Virginia
DAVID KUSTOFF, Tennessee	DWIGHT EVANS, Pennsylvania
BRIAN FITZPATRICK, Pennsylvania	BRAD SCHNEIDER, Illinois
GREG STEUBE, Florida	JIMMY PANETTA, California
CLAUDIA TENNEY, New York	JIMMY GOMEZ, California
MICHELLE FISCHBACH, Minnesota	STEVEN HORSFORD, Nevada
BLAKE MOORE, Utah	
MICHELLE STEEL, California	
BETH VAN DUYN, Texas	
RANDY FEENSTRA, Iowa	
NICOLE MALLIOTAKIS, New York	
MIKE CAREY, Ohio	

MARK ROMAN, *Staff Director*

BRANDON CASEY, *Minority Chief Counsel*

SUBCOMMITTEE ON TRADE

ADRIAN SMITH, Nebraska, *Chairman*

VERN BUCHANAN, Florida	EARL BLUMENAUER, Oregon
DARIN LAHOOD, Illinois	DAN KILDEE, Michigan
JODEY ARRINGTON, Texas	JIMMY PANETTA, California
RON ESTES, Kansas	SUZAN DELBENE, Washington
CAROL MILLER, West Virginia	DON BEYER, Virginia
LLOYD SMUCKER, Pennsylvania	LINDA SANCHEZ, California
GREG MURPHY, North Carolina	TERRI SEWELL, Alabama
GREG STEUBE, Florida	BRAD SCHNEIDER, Illinois
MICHELLE FISCHBACH, Minnesota	
DAVID KUSTOFF, Tennessee	

C O N T E N T S

OPENING STATEMENTS

	Page
Hon. Adrian Smith, Nebraska, Chairman	1
Hon. Earl Blumenauer, Oregon, Ranking Member	2
Advisory of September 20, 2024 announcing the hearing	V

WITNESSES

Robert D. Atkison, President, Information Technology and Innovation Foundation (ITIF)	3
Olivia Walch, Chief Executive Officer, Arcascope	21
Evangelos Razis, Senior Manager, Workday	27
Adrian Shahbaz, Vice President of Research and Analysis, Freedom House	38
Eric Gottwald, Policy Specialist on Trade & Economic Globalization, AFL-CIO	44

PUBLIC SUBMISSIONS FOR THE RECORD

Public Submissions	77
--------------------------	----



United States House Committee on
Ways & Means
CHAIRMAN JASON SMITH

FOR IMMEDIATE RELEASE
September 13, 2024
No. TR-06

CONTACT: 202-225-3625

**Chairman Jason Smith and Trade Subcommittee Chairman Adrian Smith
Announce Subcommittee Hearing on Protecting American Innovation by
Establishing and Enforcing Strong Digital Trade Rules**

House Committee on Ways and Means Chairman Jason Smith (MO-08) and Trade Subcommittee Chairman Adrian Smith (NE-03) announced today that the Subcommittee on Trade will hold a hearing on the importance of U.S. leadership in establishing and enforcing strong digital trade rules. The hearing will take place on **Friday, September 20, 2024, at 9:00 AM in 1100 Longworth House Office Building.**

Members of the public may view the hearing via live webcast available at <https://waysandmeans.house.gov>. The webcast will not be available until the hearing starts.

In view of the limited time available to hear the witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record can do so here: WMSubmission@mail.house.gov.

Please ATTACH your submission as a Microsoft Word document in compliance with the formatting requirements listed below, **by the close of business on Friday, October 4, 2024**. For questions, or if you encounter technical problems, please call (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission but reserves the right to format it according to guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Please indicate the title of the hearing as the subject line in your submission. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

ACCOMMODATIONS:

The Committee seeks to make its facilities accessible to persons with disabilities. If you require accommodations, please call 202-225-3625 or request via email to WMSubmission@mail.house.gov in advance of the event (four business days' notice is requested). Questions regarding accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available on the Committee website at <http://www.waysandmeans.house.gov/>.

###

PROTECTING AMERICAN INNOVATION BY ESTABLISHING AND ENFORCING STRONG DIGITAL TRADE RULES

FRIDAY, SEPTEMBER 20, 2024

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRADE,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The subcommittee met, pursuant to call, at 9:05 a.m., in Room 1100, Longworth House Office Building, Hon. Adrian Smith [chairman of the subcommittee] presiding.

Chairman SMITH. The subcommittee will come to order.

Thank you, Ranking Member Blumenauer, subcommittee members, and our witnesses for being here today. I appreciate all of you taking the time to discuss the need for U.S. leadership in establishing and enforcing strong digital trade rules.

Technology products are a crown jewel of American competitiveness. If our tech sector was its own country, its economy would be the eighth largest in the world, larger than even Canada or Russia. It employs 8.9 million Americans and pays 33 percent more than other industries on average.

However, our status as an innovation powerhouse is under threat. In recent years, our strategic and economic rivals have sought to erode America's competitive edge through a series of discriminatory digital trade and tax measures targeting American companies. There is no question this is contrary to our national interest.

This is why I was so concerned last October when the Biden administration announced it was no longer supporting core bipartisan digital trade rules in negotiations at the World Trade Organization and the Indo-Pacific.

A recent poll found 86 percent of American voters believe it is important for the U.S. to lead in writing global rules for technology. Yet where we should be leading on technology rules, America is retreating. Where we should be arguing for our values in the face of digital authoritarians, we are silent. And where we should be working with allies, we are leaving like-minded partners out to dry.

Even more concerning, it has been almost a year since USTR announced this policy change. Yet the administration has gone radio silent on what our digital trade policies should look like. Predictably, WTO partners have moved on without the United States.

At USTR's insistence, digital trade is also off the table in ongoing negotiations with Kenya, despite the chance to set a gold standard with this important partner and developing nation.

At the same time, it seems like our administration is out to lunch as foreign governments treat American companies like a piggybank by imposing new digital services taxes. It is unacceptable. Canada, one of our closest trading partners, is now collecting its DST with little response by the U.S. Government.

Make no mistake, the new USMCA dispute against Canada's DST is a positive step, but it is too little, too late. We should have been ready to act immediately when Canada proceeded unilaterally, blatantly ignoring a series of warnings from Congress and our executive branch.

Flecklessness on trade enforcement signals to foreign governments that aiming trade barriers at U.S. firms is fair game. Look no further than the European Union, which continues its regulatory assault against American Enterprise. For example, under the Digital Markets Act, six companies are designated for increased regulation as, quote, "gatekeepers." Five are American, one is Chinese, and none are European. The Digital Services Act similarly targets American innovators.

Yet the Biden administration has turned its head the other way and, in some cases, has even sent agency officials to assist the EU in implementing these laws. This sort of collusion to undermine American companies is simply unacceptable. Discriminatory actions against U.S. companies should be met with a firm response, not a helping hand.

I will close with this: America needs to return to the table. We need to get back to negotiating smart trade agreements that support our innovators; agreements with real teeth. Further, the U.S. Government must have the will to enforce them. We need to make sure foreign governments know discriminatory actions will be met with a swift and decisive response from a government that supports its job creators.

I now recognize Ranking Member Blumenauer for his opening statement.

Mr. BLUMENAUER. Thank you, Congressman Smith, for planning and organizing today's hearings. I know it has been an incredibly demanding work period with everything that is going on, and I would like to thank our panelists for joining us in the waning days of the fall session here.

In the interest of time, I will just briefly highlight a few topics that we will hear about today.

I would like to start by commending the Biden-Harris administration for their leadership role in the recent extension of the WTO e-commerce moratorium. The United States was instrumental in getting all WTO members to agree to the extension, and it was not, I am told, an easy task. The e-commerce moratorium supports American business growth and is critical to the digital economy.

Extending the e-commerce moratorium was a big priority for the Ways and Means Committee. As the chairman mentioned, the digital economy is critically important to the United States. According to the most recent data, as is mentioned, there is a tremendous amount of value that is involved with this 10 percent of the GDP,

and the digital economy grew at over 7 percent per year from 2017 to 2022.

The impressive growth for the digital economy has created new opportunities for workers, for consumers, and business. The digital economy has enabled entrepreneurs, like Dr. Walch, one of our panelists, to start small businesses that operate globally. It has led to the introduction of new technologies and platforms that have helped to drive even more innovation, improve trade facilitation, and further conservation efforts, and provide important access to telemedicine. Today, the digital economy touches most industries, whatever size.

But while the digital economy has created new opportunities and transformed certain industries, it has raised significant modern challenges. As Ambassador Tai has correctly noted, an increasingly digital and digitized economy challenges every realm of our individual and collective experience and requires careful consideration of the regulatory approach.

On the one hand, we must create conditions for a company to innovate. And yet on the other hand, we must ensure the ability of governments to regulate the digital economy, especially with respect to personal data.

In this regard, I am looking forward to hearing from Eric Gottwald today on some of these challenges both within the workplace, such as surveillance of workers, and outside the workplace, such as the erosion of personal privacy. I am concerned about that and look forward to hearing from our panelists.

Finally, I will close by noting that policymakers have an obligation to approach digital trade policy thoughtfully and deliberately. We need to strike an appropriate balance furthering the growth of the U.S. digital economy and responding to the needs of our citizens and not having them shortchanged.

I look forward to hearing from our witnesses on these issues. I appreciate, Mr. Chairman, your convening us, and look forward to a productive conversation.

Chairman SMITH. Thank you to Ranking Member Blumenauer. I appreciate your participation as well.

I would like to introduce our witnesses now. First, we will have Robert Atkinson. He is the president of the Information Technology and Innovation Foundation. We have Olivia Walch, who is the chief executive officer of Arcascope. We have Evangelos Razis, and he is the senior manager of Workday. We have Adrian Shahbaz, who is the vice president of Research and Analysis for Freedom House. And then we also have Eric Gottwald, who is the policy specialist on Trade and Economic Globalization for the AFL-CIO.

Each of you will have five minutes. You will have your timer there that you can see. Once you see that yellow light, if you could bring the flight in for a smooth landing, we would all appreciate that.

So, Dr. Atkinson, you are recognized for five minutes.

**STATEMENT OF ROBERT ATKINSON, PRESIDENT,
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION**

Mr. ATKINSON. Thank you, Chairman Smith and Ranking Member Blumenauer and members of the subcommittee. It is a

pleasure to speak with you today about this key issue that you laid out.

What is undeniable is that the U.S. leads in this sector. We have 37 percent of global market share in the IT and information services market, and it is an incredibly valuable market, and since, as you noted, pays high wages, key exports. And that is why so many foreign governments, including core allies like Canada, like Korea, and others, have targeted this sector, targeted our businesses, both in a form of digital protectionism so that they can grow their businesses. If they can hobble ours, they think they can grow their businesses to compete with ours, but also direct digital aggression. Limiting our ability to do business, taking our business company money.

And we detail in my testimony a number of key areas. And it is striking just how aggressive these areas are.

Number one, as people talk about, limiting cross-border data flows.

Number two, government-driven import substitution, where governments like the European Government are saying we don't want to buy your IT services or cloud service, we want our own. And yet Europe is running a \$200 billion trade surplus with us. And we are running a \$2 billion trade surplus in digital with them. So, essentially, they have a hundred times more trade surplus with us in other areas than we do in digital, and they won't even let us sell digital products and services to them, which is what they want to do.

Cloud center localization. You can't have your cloud data. Center has to be there.

Mandated edge provider payments to ISPs. Basically what they are doing over there is there are ISPs, there are telecom companies, they are saying, hey, we have a good idea to raise money. We will just force Amazon and Google and these other companies to just pay us money. This is a complete violation of how the internet has always worked.

Digital standards manipulation. Rather than relying on a global or voluntary standards process that we have had for decades, a lot of these countries are imposing their own standards as a way to get competitive advantage.

Digital services taxes. Mr. Smith, you mentioned that—Congressman Smith. What is important to understand that those don't come from the companies, they come from our Treasury. These companies that paid that get a tax credit against their U.S. taxes. So they are just taking tax money from U.S. taxpayers.

Aggressive antitrust against these companies. Massive fines. Particularly the Europeans, billions and billions of dollars of fines. Highest fines we have ever seen anywhere for antitrust.

Taxing streaming platforms, and giving the money to domestic companies.

And, finally, arbitrary privacy enforcement. Bringing privacy cases that would never stand in the U.S. against American companies.

So in light of all of that, it is critical that we need strong pushback against these countries. And it is unfortunate that USTR

Tai made that decision to pull out of the WTO negotiations and others to get, quote, policy space.

And I just want to close by saying, that really is not what is at stake here. Congress has the ability to do virtually anything in regulating the digital policy space. Virtually anything, as long as it doesn't discriminate in favor of American companies against foreign companies. So we could pass an AI bill if we wanted to, and it wouldn't change anything about our need to push back against foreign countries that are using AI regulation to discriminate against American companies. We could pass, and we should pass, a national privacy bill that would not at all preclude us from pushing back against cross-border data limitations.

And one of the key points that I think is lost in this debate, regulation flows with the data. The idea that if you move data offshore, you no longer have to comply with the regulatory standards of that country, is just false.

The Canadian Government brought a case a few years ago against an American company that was doing business in Canada and the U.S. It took Canadian-person data, put it into the U.S. and complied with U.S. law. Unfortunately, it broke the Canadian law. Canadians sued the company, and they won in court, as they rightly should have, because the American company violated the laws of the country they were doing business. So cross-border data flows do not mean that you can have a get-out-of-jail free card.

Let me just close by saying, this is such an important sector, as you noted, that if we don't take stronger action, we are going to lose this sector. And we are going to lose the jobs and the revenue and the exports that come with it.

So I am so pleased that you are doing this hearing because it is such a critical issue. Thank you.

[The statement of Mr. Atkinson follows:]

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 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 Komnec, “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 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'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 States, 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.

Chairman SMITH. Thank you.
Dr. Walch, you are recognized for five minutes.

**STATEMENT OF OLIVIA WALCH, CHIEF EXECUTIVE OFFICER,
ARCASCOPE**

Ms. WALCH. Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee, thank you for the opportunity to speak today. My name is Olivia Walch, and I am the CEO and founder of Arcascope, a Virginia-based company that makes software to help people sleep better by targeting their circadian rhythm.

If you have ever experienced jet lag, worked a night shift, or simply woken up in the middle of the night and not known why, you have experienced the tremendous impact that circadian rhythms can have on your sleep, health, and overall well-being. Our apps work by telling users what they need to do through personalized plans for timing their eating, light exposure, and caffeine, to start sleeping and feeling better faster.

In the time since our founding, we have had success helping users sleep better all across the United States. But our users are not just in the United States, and it is for that reason that I greatly appreciate the opportunity to speak to you all today.

Arcascope has users from countries around the world. Like most small companies, we reach these users through an infrastructure of service providers—for distribution, authentication, analytics—and each of these handle user data. The services range from as critical as handling how a user logs in to as simple as just tracking if they clicked a button. We have invested time, energy, and effort into engineering our backend to carefully handle this data.

We can't afford to constantly reengineer the backend or consult our lawyer in response to policy changes requiring us to store data locally or pay countries specific tariffs. We just lack the resources. After all, 2 weeks of my lawyer's time is half an engineer's salary. If we were in a position where the choices between redoing our backend or leaving a country whose specific rules were a compliance challenge, we would almost certainly just stop operating in that country.

And, of course, you can see the problem this poses for a jet lag app. You don't want to take off from Dulles and not have your app work in Delhi.

We already limit the data we collect because of compliance headaches. If you land in Delhi and you want to know why we are telling you not to drink coffee, I can't tell you without having you go to settings and export a diagnostic report and email it to us, which is a hassle. And it is caused by disparate regulations we encounter around the globe.

If the fracturing of digital trade is allowed to continue, I am confident that established third-party providers will sell us compliance for a price, passing their costs on to us, and further entrenching the already big players in the technology space. Compliance with countless nation-specific digital trade laws takes a lot of lawyers, and there aren't that many companies with lawyers at the scale of Meta, Google, Amazon. We are not one of those.

I want to briefly touch on the e-commerce moratorium, source code disclosure, and data flows with my remaining time.

Digital goods are, essentially, information, which makes them inherently different from trade and physical goods. And I am grateful for the WTO e-commerce moratorium in place right now which makes it so that digital goods are not subject to tariffs in the same way physical goods are. And it is from this place of gratitude that I call for strong U.S. leadership to continue the moratorium and ultimately make it permanent.

As a startup, putting our proprietary innovations at risk is putting our entire company at risk. Requirements to share source code as part of operating in that country would mean exposing our secret sauce to foreign regulators that probably don't have our best interests in mind. Our only option would again be to stop operating in a country that demanded that.

And it is easy to see how the imposition of localization requirements would be stifling to products like our jet lag app, but almost any business would be disrupted by barriers to cross-border data flows. And despite the tendency to think of tech as nice to have, like social media or streaming services, data flows can be critical and life-sustaining.

My company's ambitions go far beyond our jet lag app. We are the first mover in the field of consumer chronomedicine, timing drugs so that they are maximally effective and minimally toxic. Drugs like chemotherapy.

We work with researchers around the world, and we need to be able to share data with each other. Innovation will happen fastest if barriers to data flows across borders are kept as frictionless as possible. There are good reasons for slowdowns and sharing of health data to occur, like rigorous human subjects and privacy protections. But inconsistent, nation-specific, trade bureaucracy is not one of them.

U.S. small businesses like mine need strong leadership to prevent rules like tariffs on digital goods, mandatory data localization, enforced source code disclosure from hampering our global growth.

With strong leadership on digital trade from the United States, companies like Arcascope can continue to do what we do best, which is build and compete on a global stage. And we can continue to help you avoid jet lag on your next congressional delegation.

Thank you for the opportunity to speak today, and I look forward to your questions.

[The statement of Ms. Walch follows:]



Testimony of Dr. Olivia Walch
CEO and Founder of Arcascope

Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Trade

September 20, 2024

Chairman Smith, Ranking Member Neal, Chairman Smith, Ranking Member Blumenauer, and members of the Subcommittee, thank you for the opportunity to speak today. My name is Olivia Walch, and I am the CEO and founder of Arcascope, a Virginia-based company that makes software to help people sleep better by targeting their circadian rhythms. If you've ever had jet lag, worked a night shift, or simply woken up in the middle of the night and not known why, you've experienced the tremendous impact circadian rhythms can have on your sleep, health, and overall wellbeing. Arcascope's apps work by telling our users what they need to do—through personalized plans for timing their eating, light exposure, and caffeine—to start sleeping and feeling better, faster.

I first started making apps while working on my PhD in Applied Mathematics at the University of Michigan. At the time, I was borrowing a school computer and coding at the kitchen table of the apartment I shared with three roommates. While learning to code in Objective C was miserable and the chairs weren't comfortable, the act of making something and being able to share it with the world from a kitchen table was incredible. I've been addicted to that feeling ever since. It's what led me to apply for Small Business Innovation Research (SBIR) grants from the National Institutes of Health after I graduated, and it's what drove me to raise \$3M in angel and venture funding after we leveraged our SBIR funds to run a successful clinical trial showing efficacy of our technology.

I still work at a kitchen table, even though I have a much more comfortable chair these days. Arcascope now employs six people, remotely distributed across the U.S. In the time since our founding, we've had success helping users sleep better all across the United States.

But our users are not *just* from the United States.

It's for that reason that I greatly appreciate the opportunity to share our perspective on digital trade, data flows, and the eCommerce moratorium today.

Operating globally as a small business

Arcascope has users from countries around the world. Like most small companies, we reach these users through an infrastructure of service providers—for distribution, subscription processing, authentication and analytics—that each handle user data. The services range from as critical as handling how users login to as simple as tracking which buttons they click. We've invested time, effort, and energy into engineering our backend to carefully handle this data.

We can't afford to constantly re-engineer this backend or consult our lawyer in response to policy changes requiring us to store data locally or pay country-specific tariffs—we lack the resources. After all, two weeks of our lawyer's time is half an engineer's salary. If we were in a position where the choice was redoing our backend or leaving the country whose specific rules were presenting a compliance challenge, we would almost certainly just stop operating in that country.

Of course, you can probably see the problem this poses for a jet lag app. No one wants to use a jet lag tool that works when you take off from Dulles but doesn't when you land in Delhi.

We already limit the data we collect, even though it would be useful, to avoid compliance headaches in places like India. If you step off the plane in Delhi, and our app is telling you to avoid caffeine after 8:45 am, you might

wonder why. But we can't explain to you why the app is saying that unless you go to settings, export a diagnostic report for us, and email it in—a hassle for all involved—and caused by the disparate regulations we encounter around the globe.

If the fracturing of digital trade is allowed to continue, established third party providers will sell us compliance, for a price—passing their compliance costs on to us—and further entrenching the already-big players in the technology space. After all, compliance with countless, nation-specific digital trade rules takes a lot of lawyers, and there aren't that many companies with legal resources on the scale of Amazon, Meta, and Google.

Sharing information is not like shipping shoes

Digital goods are, essentially, information, which makes them inherently different from trade in physical goods like shoes. Existing frameworks like the WTO eCommerce moratorium recognize that electronically transmitting information shouldn't be taxed.

Imagine that I'm on the phone with a friend in Indonesia, helping her overcome her jet lag. I factor in when she slept last, her light exposure, and her recent activity, to tell her what she should do during the day to feel better faster.

It's a phone call, so there are no digital goods, and there wouldn't be any digital tariffs involved.

But what if I sent an audio file of myself saying the same information? Or put it in a PDF? Or what if, instead of *me* telling her what to do, I used an algorithm trained on the kind of advice I typically give to create the recommendations? And what if I accessed that algorithm via an app?

Or, to really drive this point home: what if I took the binary source for that app and read the ones and zeros out loud to my friend over the phone, so she could recreate the entire app from scratch on her own computer? (This would take a long time, and hopefully she'd be over her jet lag by the time we finished, but the point still stands).

In each one of these cases, the *information* being shared is identical, but the tariff implications could be wildly different if digital transmissions could be taxed. Information should not be subject to tariffs in some forms but not others.

The small business owner in me is grateful that, thanks to the WTO eCommerce moratorium in place right now, digital goods *are not* subject to tariffs in the same way as physical goods. It's from this place of gratitude that I call for strong U.S. leadership to continue the moratorium and ultimately make it permanent.

Data flows foster innovation

It's easy to see how the imposition of localization requirements would be stifling to products like our jet lag app. But almost any business would be disrupted by barriers to cross-border data flows. And despite the tendency to think of tech as nice-to-haves, like social media or streaming services, data flows can be critical and life-sustaining.

My company's ambitions are much larger than helping people feel better after an international trip. We're the first mover in the field of commercial chronomedicine, or circadian medicine—helping people time drugs in ways that are personalized to them so that the drugs are more effective and less toxic. Researchers around the world have seen staggering results, including the finding that certain drugs can cause tumors to shrink when given at some times and grow at an accelerated rate when given at other times. In other words, timing your drug wrong could be worse than not even taking it at all.

My company and I are working with researchers around the world—in Korea, Italy, the United Kingdom, Germany. We need to be able to share data with each other. Innovation will happen fastest if barriers to data flows across borders are kept as frictionless as possible. There are good reasons for slowdowns in sharing of health data to occur, like rigorous human subjects and privacy protections. Nation-specific trade bureaucracy is not one of them.

Sharing source code is a non-starter

As a start-up, putting our proprietary innovations at risk is putting our entire company at risk. Requirements to share source code as part of operating in a country would mean exposing our "secret sauce" to foreign regulators that probably do not have our interests—or U.S. interests—in mind. Undermining our business and our competitiveness in that way is not a risk we can afford. Again, our only option would be to stop operating in that country.

That does not mean innovation in circadian timing won't happen there. It means a non-U.S. competitor or someone better-funded and with more legal resources will beat us to it.

Conclusions

U.S. small businesses like mine need strong leadership to prevent rules like tariffs on digital goods, mandatory data localization, or forced source code disclosure from hampering our global growth.

My company originated in a first-floor apartment about 500 feet from Michigan Stadium. I was able to grow my company thanks to SBIR funding, access to top-level talent, and an unparalleled innovation ecosystem. The United States is the best place in the world for small tech. But my company cannot invest resources to retool our product for a fractured trade environment in the same way that larger companies can.

Without proactive digital trade leadership from the United States, the already entrenched players will become more entrenched and global markets that U.S. startups like mine can reach will become smaller. With strong leadership on digital trade from the United States, companies like Arcascope can continue to do what we do best—build—and compete on a global stage. And we can continue to help you avoid jet lag on your next Congressional Delegation.

Thank you for the opportunity to speak today, and I look forward to your questions.

Chairman SMITH. Thank you.
Mr. Razis, you are recognized for five minutes.

**STATEMENT OF EVANGELOS RAZIS, SENIOR MANAGER,
WORKDAY**

Mr. RAZIS. Good morning, Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee. My name is Evangelos Razis, and I am senior manager of public policy at Workday, where I lead our policy efforts on data flows, privacy, and AI.

Workday is a leading provider of enterprise cloud applications for finance and H.R. Our software is used by more than 10,000 organizations around the world and across industries, including more than 60 percent of the Fortune 500. There are 70 million workers in the Workday customer community, and nearly 30 percent of all U.S. job openings are processed using our software.

I commend the subcommittee for its bipartisan focus on strong digital trade rules and would like to offer three points for my written testimony.

First, digital trade rules are vital for cross-border data flows, which Workday and our customers rely on to grow, innovate, and do business. Workday can develop AI-powered solutions here in the United States and deliver them to our customers wherever they are in the world.

Chairman SMITH. Mr. Razis, could you pull your microphone a little closer? Thank you.

Mr. RAZIS. Enterprises in every major industry, from manufacturing to retail to financial services, rely on our software platform to recruit, manage, train, and empower their employees, complete payroll, process benefits, and manage their finances. Unfortunately, barriers to the free flow of information and digital services exports are growing abroad.

For cloud software companies like Workday and our customers, data localization requirements are particularly challenging. Unlike legacy systems, cloud software like Workday runs on third-party infrastructure and is delivered through the internet. Customers get the benefit of our software without having to purchase, install, update, and manage it. This business model was pioneered in the United States, and it enables companies in every sector of the economy to access innovative new technologies, including AI, securely and on scale.

Second, strong digital trade rules complement and don't preempt smart regulations. Workday sees incredible opportunities for technology to unlock human potential, but we also recognize that people won't use technology they don't trust. For this reason, we support robust privacy protections. And whether it is Federal privacy reforms or comprehensive State privacy laws, one thing is clear, no leading U.S. privacy framework runs afoul of strong digital trade rules because they don't impose the kinds of data localization requirements and data transfer restrictions that digital trade rules target. Workday also supports smart regulation on high-risk uses of AI. We have endorsed legislation here in Congress that would advance meaningful AI governance.

As with privacy, AI frameworks like the first in the Nation, Colorado AI Act, don't violate digital trade rules. Why? Because they don't require foreign companies to transfer source code as a condition for doing business. Put differently, we don't face a choice of strong digital trade rules, rigorous privacy protections, or smart AI regulation. We can and we should choose all of the above.

Third, far from undermining domestic regulations, strong digital trade rules support global regulatory cooperation and better protect consumers. Under the USMCA and the U.S.-Japan Digital Trade Agreement, which are the gold standards, governments commit to having laws that protect privacy and address fraudulent and deceptive practices online.

At a time when trade barriers are erected in the name of privacy, cybersecurity, and other policy aims, digital trade rules advance a vision of a trustworthy and open economy.

Like many, we were surprised by USTR's decision last year to withdraw support for strong digital trade rules at the WTO. U.S. leadership sets the tone around the world on data policy, and USTR's decision cedes crucial ground on a growing number of trade barriers abroad.

In closing, I am grateful for the opportunity to testify before the subcommittee. Workday, as well as our customers and their employees, benefit greatly from U.S. leadership in this space. As you chart a way forward on digital trade, the subcommittee can consider us a partner and ally in its efforts.

Thank you.

[The statement of Mr. Razis follows:]



U.S. House Committee on Ways and Means

Trade Subcommittee

“Protecting American Innovation by Establishing and Enforcing Strong Digital
Trade Rules”

Written Testimony of Evangelos Razis

Senior Manager, Public Policy

Workday

September 20, 2024

Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee. On behalf of Workday, thank you for the opportunity to share our views on the synergies between strong digital trade rules, cross-border data flows, and smart technology regulation. I commend the subcommittee for convening today's hearing and for its bipartisan focus on U.S. leadership in digital trade in a challenging global environment.

My name is Evangelos Razis, and I'm Senior Manager of Public Policy at Workday, where I lead the company's policy efforts on data flows, privacy, and artificial intelligence (AI). My colleagues and I engage with federal and state policymakers to support workable, meaningful, and risk-based frameworks that build trust in digital technologies. Previously, I led digital trade and international data policy at the U.S. Chamber of Commerce, advocating around the world for U.S. exporters of all sizes and in every industry. Throughout my career, I have seen, first hand, the importance of U.S. leadership on digital trade in promoting and protecting American innovation.

Background

Workday is a leading provider of enterprise cloud applications for finance and human resources.¹ Founded in 2005, Workday offers companies a single cloud-native platform to help them manage their most important assets: their people and money.

Today, Workday is used by more than 10,500 organizations around the world and across industries, from medium-sized businesses to more than 60% of the Fortune 500. Headquartered in Pleasanton, California, we have nearly 20,000 employees and offices across the U.S., including in Atlanta, Boulder, Chicago, Dallas, McLean, Minneapolis, and Seattle. Our customers' employees are a community of more than 70 million Workday users, and in the first half of 2024 nearly 30% of all U.S. job openings were processed using our software.² We are deeply committed to providing innovative, reliable, and secure software services to our customers and their employees. We also believe we have a unique opportunity to improve employee experiences and empower people to do their best work.

For Workday and our customers, digital trade is essential for exporting to foreign markets and engaging in day-to-day global commerce. Our software platform is available in 35 languages and more than 175 countries, enabling enterprises and their employees to work seamlessly across borders. With 75% of our business in North America, access to foreign markets is essential for our continued growth.³

¹ "Company Overview," Workday Newsroom, <https://newsroom.workday.com/company-overview>.

² "Workday Global Workforce Report: Restoring Trust Before Your Top People Leave," Workday, 2024, https://forms.workday.com/en-us/reports/workday-global-workforce-report/form.html?step=step1_default.

³ Esherwood, P., "New Dawn, new Workday: Carl Eschenbach to lead next chapter," ERP Today, <https://erp.today/new-dawn-new-workday-carl-eschenbach-to-lead-next-chapter/>.

My testimony will focus on the importance of high-standard digital trade rules for cross-border data flows, which Workday and our customers rely on to grow, innovate, and do business around the world. I will also discuss the importance of smart regulations that build trust in the digital economy, especially with regard to data privacy and AI. We believe high-standard digital trade rules complement smart regulations and advance global regulatory cooperation, which promotes U.S. interests and better protects consumers.

I. U.S. leadership on digital trade is vital for cross-border data flows, which Workday and our customers rely on to grow, innovate, and do business.

Since the 1990s, the U.S. has led the world in advocating for rules, frameworks, and norms that advance an open digital economy.⁴ While this longstanding policy approach reflects American values and supports a variety of U.S. interests, the economic benefits are clear.⁵ The U.S. is the world's largest exporter of cross-border services, and digitally-enabled exports drive much of the U.S.'s \$1 trillion services trade surplus.⁶ A study published this spring found that digital trade supports 3 million American jobs.⁷ As a U.S.-headquartered company supporting thousands of U.S. enterprises, and whose platform is used by millions of American workers every day, we are proud to contribute to the U.S.'s considerable digital-trade advantage.

For decades, policymakers in Congress and the executive branch from both parties have sought to preserve this advantage through enforceable trade rules. In 2001, the U.S. entered its first trade agreement with commitments on electronic commerce.⁸ Previous administrations built on these efforts, culminating in the high-standard disciplines in the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement (USJDTA). Today, these disciplines are the gold standard. The USMCA and USJDTA safeguard the free flow of information across

⁴ E.g., "A Framework For Global Electronic Commerce," The White House, July 1, 1997, <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>; "The Geneva Ministerial Declaration on global electronic commerce," World Trade Organization, May 18, 1998, https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.

⁵ See "Cross-Border Data Policy Index," Global Data Alliance, <https://globaldataalliance.org/resource/cross-border-data-policy-index/>.

⁶ "What Drives the U.S. Services Trade Surplus? Growth in Digitally-Enabled Services Exports," The White House, June 10, 2024, <https://www.whitehouse.gov/cea/written-materials/2024/06/10/what-drives-the-u-s-services-trade-surplus-growth-in-digitally-enabled-services-exports/>; "Recent Trends in U.S. Services Trade: 2024 Annual Report," United States International Trade Commission, May, 2024, <https://www.usitc.gov/publications/332/pub5512.pdf>.

⁷ Heiber, J. and Icsó, I., "How Digital Trade Benefits the American Economy," U.S. Chamber of Commerce, March 19, 2024, <https://www.uschamber.com/international/trade-agreements/how-digital-trade-benefits-the-american-economy>.

⁸ "Agreement Between the United States Of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area," October 24, 2000, <https://ustr.gov/sites/default/files/Jordan%20FTA.pdf>.

borders and ban market access barriers, including data localization requirements and mandates to transfer source code and algorithms as a condition for doing business.⁹ The rules in these agreements have only grown in importance because of rapid advances in AI.

Like many, we were surprised by the U.S. Trade Representative's (USTR) decision last year to withdraw support for high-standard digital trade rules at the World Trade Organization (WTO).¹⁰ U.S. leadership sets the tone around the world on data policy, and USTR's decision cedes crucial ground to the growing number of digital trade barriers erected abroad. It also appears at odds with the current administration's efforts to promote a freer and more secure internet and build "digital solidarity" with U.S. allies and partners.¹¹ Safeguarding cross-border data flows and protecting exporters from market access barriers has long been a bipartisan priority. We applaud committee members' recent expressions of support for high-standard digital trade rules, which are necessary in a challenging global environment.

For Workday, high-standard digital trade rules safeguard our ability to export innovative and secure software services abroad. The ability to transfer data and access information across borders is essential. Workday can develop AI-powered solutions in the U.S. and deliver them digitally to our customers, wherever they are in the world. While Workday is a technology company, enterprises in every major industry rely on our software platform to recruit, manage, train, and empower their employees; complete payroll; process benefits; and manage their finances. Workday can deliver services securely and in a privacy-protective way because of legal, technical, and administrative measures that are the cornerstone of the enterprise cloud software industry.¹²

The U.S. has multiple avenues for advancing the free flow of information and promoting open markets. Bilateral agreements, such as the U.S.-EU Data Privacy Framework, and multilateral initiatives at the Organization for Economic Cooperation and Development (OECD), among other fora, are vital for building trust in the digital economy.¹³ Yet they are not sufficient for

⁹ United States-Mexico-Canada Agreement, Chapter 19: Digital Trade, December 10, 2019, <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>; United States-Japan Digital Trade Agreement, October 7, 2019, <https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text>.

¹⁰ "USTR Statement on WTO E-Commerce Negotiations," Office of the United States Trade Representative, October 24, 2023, <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations>.

¹¹ See "National Cybersecurity Strategy," The White House, March, 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>; "A Declaration for the Future of the Internet," The White House, April, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf; "United States International Cyberspace & Digital Policy Strategy," U.S. Department of State, May, 2024, <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>.

¹² "Trust," Workday, <https://www.workday.com/en-us/why-workday/trust/overview.html>.

¹³ "Data Privacy Framework (DPF) Overview," Data Privacy Framework Program, <https://www.dataprivacyframework.gov/Program-Overview>; <https://www.oecd.org/en/about/programmes/data-frec->

safeguarding U.S. exports of digitally-enabled goods and services. High-standard digital trade rules, together with enforcement, can open and sustain market access for American companies in all sectors of the economy.¹⁴

U.S. leadership on digital trade is needed now more than ever. Barriers to the free flow of information and exports of U.S. digitally-enabled services are growing abroad.¹⁵ One study in 2021 found that 62 countries implemented 144 data localization requirements, up from only 35 countries and 67 such barriers in 2017.¹⁶ Until recently, the National Trade Estimate (NTE), an annual report compiled by USTR at Congress's direction, comprehensively identified and analyzed these growing barriers to digital trade.¹⁷ Although USTR has limited its reporting on data localization requirements in the most recent NTE, persistent trend lines suggest the global environment has gotten more—not less—challenging.¹⁸

Workday is better positioned than many to overcome market access barriers. For small businesses, these barriers can halt digitally-enabled exports altogether.¹⁹ At the same time, data localization requirements can be particularly challenging for cloud software companies. In fact, Workday launched its policy advocacy efforts in 2018 in response to threats to cross-border data flows. Unlike legacy systems, where customers use software on their own on-premises data centers, cloud software services are delivered through the internet. This “software-as-a-service” business model was pioneered in the U.S., and it enables companies in every sector of the

flow-with-trust.html ; “Data free flow with trust,” Organisation for Economic Co-operation and Development, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

¹⁴ For example, U.S. manufacturers are the second-largest exporter of digitally-enabled services. “What Drives the U.S. Services Trade Surplus?”

¹⁵ See “OECD Services Trade Restrictiveness Index,” Organisation for Economic Co-operation and Development, February 12, 2024, https://www.oecd.org/en/publications/oecd-services-trade-restrictiveness-index_b9e5c870-en/full-report.html#introduction-d5e23.

¹⁶ Cory, N. and Dascoli, L., “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,” Information Technology & Innovation Foundation, July 19, 2021, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

¹⁷ See “Joint Association Memorandum to Members of the Senate Committee on Finance and House Committee on Ways and Means,” April 12, 2024, <https://www.nftc.org/wp-content/uploads/2024/04/Joint-Association-Memo-on-2024-NTE-Digital-Trade-Barrier-Report.pdf>.

¹⁸ See “The Extent and Impact of Data Localisation,” Frontier Economics, June 1, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf.

¹⁹ See “Cross-Border Data Transfers & Small Businesses,” Global Data Alliance, <https://globaldataalliance.org/issues/small-businesses/>; Icsa, I., “How USTR’s Digital Trade Reversal Will Hurt Small Businesses,” U.S. Chamber of Commerce, November 20, 2023, <https://www.uschamber.com/international/trade-agreements/ustr-digital-trade-reversal-will-hurt-small-businesses/>; “Making Small Businesses Mighty: The Digital Trade Opportunity for Small Businesses in the Indo-Pacific,” Global Innovation Forum, September, 2022, <https://globalinnovationforum.com/reports/us-apac-small-business-digital-trade/>.

economy to access innovative new technologies, including AI, securely and at scale. By contrast, data localization can mean fewer and costlier services that are less innovative and less secure.²⁰

II. High-standard digital trade rules complement smart regulations which, together, build trust in the digital economy.

For Workday and others, USTR’s decision last year was also surprising for its rationale, the need for “policy space” to regulate the digital economy. International trade rules safeguard exporters from arbitrary and discriminatory restrictions enacted by foreign governments. They do not preempt domestic regulation, regardless of whether the law is already in force or has yet to be enacted. Under the General Agreement on Trade in Services, USMCA, and the USJDTA, governments have a right to regulate their domestic economies.²¹ Moreover, when Congress passed USMCA’s implementing legislation by an overwhelming bipartisan majority, it reiterated that U.S. law prevails if there is any conflict with the agreement’s disciplines.²² This provision is standard in U.S. trade law.²³

Workday actively supports both high-standard digital trade rules and smart technology regulations. We see incredible opportunities for technology to unlock human potential. But we also recognize that the risk of unintended consequences is real and that people won’t use technology they don’t trust. Smart regulations can address this trust gap.²⁴ For these reasons, Workday advocates for workable, meaningful, and risk-based frameworks for the digital economy at the federal level, in state capitals, and in markets around the world. *In our view, high-standard digital trade rules complement—and don’t preempt—these regulations.* Our experience with data privacy and AI governance illustrates why.

- **Data Privacy Protections:** Workday views privacy as a fundamental human right.²⁵ As a California-headquartered company with operations in the European Union, we must comply with the California Consumer Privacy Act and the General Data Protection Regulation (GDPR), among other leading frameworks. Workday also uses government-

²⁰ “The ‘Real Life Harms’ of Data Localization Policies,” Centre for Information Policy Leadership, March, 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf.

²¹ See Article XIV of the General Agreement on Trade in Services, which is incorporated in both the U.S.-Mexico Canada Agreement (Article 32.1(2)) and U.S.-Japan Digital Trade Agreement (Article 3(1)).

²² USMCA Implementation Act, Pub. L. 116-113, Section 102 (Relationship of the USMCA to United States and State Law); S. Rep. 116-283 at 40 (confirming that “U.S. law prevails in the case of a conflict with the USMCA.”).

²³ E.g., United States-Korea Free Trade Agreement Implementation Act, Pub. L. 112-41, Section 103 (Relationship of the Agreement to United States and State law) and United States-Panama Trade Promotion Agreement Implementation Act, Pub. L. 112-43, Section 102 (Relationship of the Agreement to United States and State law).

²⁴ “Workday Global Survey Reveals AI Trust Gap in the Workplace,” Workday Press Release, January 10, 2024, <https://investor.workday.com/2024-01-10-Workday-Global-Survey-Reveals-AI-Trust-Gap-in-the-Workplace>.

²⁵ “Privacy at Workday,” Workday, <https://www.workday.com/en-us/why-workday/trust/privacy.html>.

backed tools for transferring personal information across borders in a privacy-protective way.²⁶ These include the U.S.-EU Data Privacy Framework, the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules System, binding corporate rules, and standard contractual clauses. We invest in these data transfer tools to provide our customers and their employees with assurance that their personal information is protected.²⁷

We also support a federal comprehensive privacy law that protects U.S. consumers and enables responsible innovation.²⁸ Federal privacy reform is long overdue. In recent years, there have been two bipartisan, bicameral attempts to advance U.S. privacy protections: the American Data Privacy and Protection Act (ADPPA) and the American Privacy Rights Act (APRA).²⁹ Both bills would require rigorous protections on personal information. Neither would impose the kinds of discriminatory data localization requirements or restrictions on cross-border data transfers that high-standard digital trade rules prohibit. The same can be said of sectoral privacy laws at the federal level and the comprehensive privacy laws enacted by nineteen states.³⁰ Indeed, data localization has been shown to harm the privacy and security of consumers' personal information.³¹ The binary choice between high-standard digital trade rules and rigorous privacy protections is a false one.

- **Risk-Based AI Regulation:** Given recent progress in AI development, lawmakers around the world are also considering whether to institute new safeguards to protect consumers. Workday has endorsed bipartisan, bicameral legislation here in Congress that would advance meaningful AI governance, and we are active in state capitals in support

²⁶ Cosgrove, B., "Workday's Take on Global Data Transfers: An Update and What's Next," Workday Blog, May 12, 2022, <https://blog.workday.com/en-us/workdays-take-global-data-transfers-update-whats-next.html>.

²⁷ Cosgrove, B., "What the New EU-US Data Privacy Framework Means for Cross-Border Data Transfers," Workday Blog, July 10, 2023, <https://blog.workday.com/en-us/what-new-trans-atlantic-executive-order-a-cross-border-data-transfers.html>.

²⁸ "Accounting for Enterprise Cloud Technologies in Comprehensive U.S. Privacy Legislation," Workday, 2019, <https://www.workday.com/content/dam/web/en-us/documents/whitepapers/privacy-accounting-for-enterprise-cloud.pdf>.

²⁹ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024).

³⁰ See Folks, A., "US State Privacy Legislation Tracker," International Association of Privacy Professionals, July 22, 2024, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

³¹ Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*, 1–32. <https://doi.org/10.1080/23738871.2024.2384724>; Swire, Peter and Kennedy-Mayo, DeBrae, The Effects of Data Localization on Cybersecurity - Organizational Effects (June 15, 2023). Georgia Tech Scheller College of Business Research Paper No. 4030905. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.4030905>; Shahbaz, A., Funk, A., & Hackl, A., "User Privacy or Cyber Sovereignty?," Freedom House, July, 2020, <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>.

of AI regulation.³² Notably, in May, Colorado passed a first-in-the-nation law to regulate high-risk uses of AI.³³ Similar to state comprehensive privacy laws, the ADPPA, and an early version of APRA, the Colorado AI Act aims to protect consumers from AI-related harms such as unlawful discrimination.³⁴ These federal and state frameworks do not run afoul of USMCA or the USJDTA, including the agreements' protections for American innovators' source code and algorithms.

Why? Because federal and state AI frameworks do not require foreign companies to transfer intellectual property as a condition for doing business. In fact, the Colorado AI Act and ADPPA provide for trade secrets protections.³⁵ They are also enforced by regulators that are empowered to demand information about AI systems to investigate potential violations—the same practices that are expressly exempted from USMCA and USJDTA's disciplines on source code and algorithms.³⁶

Workday is not alone in believing that high-standard digital trade rules complement—rather than preempt—technology regulations. U.S. allies and partners do as well. Japan, which is a leading advocate for digital trade rules, has a modern, comprehensive data privacy law and is an important convenor on global AI governance.³⁷ The same is true of the United Kingdom, which has the GDPR and is considering new AI regulations.³⁸ In recent years, the EU has also made commitments to new digital trade disciplines.³⁹ Put differently, the U.S. allies and partners that have been the most active in regulating the digital economy recognize that domestic technology regulation is consistent with digital trade rules.

³² “Reps Lieu, Nunn, Beyer, Molinaro Introduce Bipartisan Bill To Establish AI Guidelines For Federal Agencies And Vendors,” Congressman Don Beyer Press Release, January 10, 2024, <https://beyer.house.gov/news/documentsingle.aspx?DocumentID=6066>.

³³ Colorado Artificial Intelligence Act, Senate Bill 24-205, 2024, <https://leg.colorado.gov/bills/sb24-205>.

³⁴ See Rice, T., Francis, J., & Lamont, K., “U.S. State AI Legislation: How U.S. State Policymakers Are Approaching Artificial Intelligence Regulation,” Future of Privacy Forum, September, 2024, <https://fpf.org/blog/fpf-unveils-report-on-emerging-trends-in-u-s-state-ai-regulation/>.

³⁵ Colorado AI Act, Section 6-1-1703(8) ; ADPPA, Section 207(c)(3)(B)(ii).

³⁶ USMCA, Article 19.16 ; USJDTA Article 17.

³⁷ Japan Act on the Protection of Personal Information, Act No. 57 of 2003, <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en> ; “Hiroshima AI Process,” <https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html>.

³⁸ United Kingdom Data Protection Act 2018, <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> ; Coulter, M., “Britain’s new government aims to regulate most powerful AI models, Reuters, July 17, 2024, <https://www.reuters.com/technology/artificial-intelligence/britains-new-government-aims-regulate-most-powerful-ai-models-2024-07-17/>.

³⁹ “EU and Japan conclude landmark deal on cross-border data flows at High-Level Economic Dialogue,” European Commission Press Release, October 28, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378 ; EU-UK Withdrawal Agreement, European Commission, November 12, 2019, https://commission.europa.eu/strategy-and-policy/relations-united-kingdom/eu-uk-withdrawal-agreement_en.

III. High-standard digital trade rules support global regulatory cooperation and better protect consumers.

Far from undermining domestic regulations, high-standard digital trade rules promote consumer protection and cross-border regulatory cooperation. Under the USMCA and the USJDTA, governments commit to adopting or maintaining laws that protect privacy and address fraudulent and deceptive practices online.⁴⁰ Parties to USMCA also agree to exchange information and cooperate when regulating digital technologies and enforcing the law.⁴¹

In addition to protecting consumers, global regulatory cooperation enabled through high-standard digital trade rules advances U.S.-supported frameworks, including the National Institute for Standards and Technology's Cyber Security Framework, the APEC Privacy Framework, and OECD recommendations.⁴² At a time when discriminatory and arbitrary trade barriers are erected in the name of privacy, cybersecurity, and other policy aims, a U.S. vision for cultivating a trustworthy and open digital economy is needed. Without high-standard digital trade rules, the U.S. loses a key avenue for promoting its values and interests abroad, including the interests of U.S. digital services exporters and the millions of workers they employ.

U.S. leadership on digital trade is vital for maintaining the global free flow of information and an open digital economy. When the U.S. led on digital trade, our closest allies and partners joined to develop and commit to high-standard rules. Today, these countries—Australia, Japan, the United Kingdom, and Singapore, among others—have been crucial in supporting rules that align with U.S. values and interests.⁴³ Unfortunately, USTR's decision isolates the U.S. at a moment when data localization requirements and other foreign trade barriers continue to grow. If the U.S. cedes leadership, the impacts will be felt not only by businesses and employees, but by everyone who seeks a free and open internet and an “innovative, secure, and rights-respecting digital future.”⁴⁴

Conclusion

Again, I am grateful for the invitation to testify before the subcommittee. At Workday, we believe that high-standard digital trade rules and smart regulations on digital technologies are not only consistent but complementary. As an enterprise cloud software company, Workday, as well as our customers and their employees, benefit greatly from U.S. leadership in this vital space. As you chart a way forward on digital trade, the subcommittee can consider us a partner and ally in its efforts.

⁴⁰ USMCA, Article 19.7-19.8 ; USJDTA, Article 14-15.

⁴¹ USMCA, Article 19.14.

⁴² USMCA, Article 19.8(2), (6); USMCA, Article 19.15; USJDTA, Article 19.

⁴³ Declaration for the Future of the Internet.

⁴⁴ Cyberspace & Digital Policy Strategy.

Chairman SMITH. Thank you, Mr. Razis.
Mr. Shahbaz.

**STATEMENT OF ADRIAN SHAHBAZ, VICE PRESIDENT OF
RESEARCH AND ANALYSIS, FREEDOM HOUSE**

Mr. SHAHBAZ. Thank you.

Chairman Smith, Ranking Member Blumenauer, members of the subcommittee, it is an honor to testify before you today. My name is Adrian Shahbaz. I am the vice president for research at Freedom House. We are a nonprofit and nonpartisan organization founded in 1941. Our mission is to protect and expand freedom around the world.

I am grateful to this subcommittee for elevating the human rights angle of digital trade. The protection of fundamental freedoms is necessary for upholding a rule-of-law system that protects innovation and enables both prosperity and security. My remarks will draw on Freedom House's annual Freedom on the Net report, which assesses internet freedom in over 70 countries.

We work with local experts to produce country reports and scores on obstacles to access, limits on content, and rights violations. The project is widely used by public and private sectors to understand global regulatory developments, assess operational and human rights risks, and set internal priorities and policies.

Let me say we have been honored to have Members of Congress from both sides of the aisle provide opening remarks at our report launches.

A free and open internet is crucial, not only for political participation and free expression, but also for commerce, healthcare, and education. With the right tools, a schoolteacher in my father's home country of Afghanistan can access the same information and learning platforms as a student in Washington, D.C. This is due to the way that the internet is run as a global, decentralized network where information and data flow across borders. But authoritarian governments are on a campaign to change that, and in their own countries and on the international stage, we see increased moves to divide the global internet into national networks that are more easily controlled.

For these reasons, we expressed concern 1 year ago when the United States Trade Representative dropped support for cross-border data flows at the World Trade Organization. The decision risks further fragmenting the global internet by emboldening authoritarian governments to enact data localization laws. These laws require companies and other service providers to store data about local residents on service within the country. And while they are often passed another premise of growing the digital economy or protecting users' privacy, research has shown that data localization can actually hinder growth and impair cybersecurity tools.

Our own research has found that these laws can have negative implications for people's freedoms, particularly in countries that are ranked partly free and not free in our annual report. That is because data localization laws are often used to force companies to comply with local security agencies, including to censor nonviolent, political, social, and religious speech, and to hand over personal data.

One of the clearest examples is China, which has received the worst score in our net freedom index for 9 consecutive years. Vague provisions and several laws mandate that the companies collect and store their data within China's borders and that companies assist the Chinese Government with national security and intelligence efforts.

Given China's dismal human rights record, these laws put companies at a high risk of complicity with serious human rights abuses. The Chinese Communist Party considers all sorts of non-violent political, social, and religious expression as a threat to national security. And we know that they rely on technology companies to conduct mass surveillance of Uyghurs and other persecuted ethnic and religious communities.

Chinese officials have also partnered with Russia to reshape global cyber norms at the United Nations and other fora. They seek to make the world safe for authoritarianism by affirming the right to curtail the political rights and civil liberties of their own people online and off.

If global norms shift further away from a freedom and openness, there is a risk that data localization laws will proliferate, companies in authoritarian countries will face increased demands to comply with human rights abuses, and billions of people around the world will become less free.

The United States plays a critical role in preserving a free flow of information and data across borders. A necessary condition, not only for the protection of freedom, but for advancing innovation, prosperity, and security.

To ensure the United States continues its leadership role, Congress should, one, urge the executive branch to advance the goals outlined in the U.S. International Cyberspace and Digital Policy Strategy; namely, to quote, "develop shared mechanisms that will help maintain an open, interoperable, secure, and reliable internet, as well as trusted cross-border data flows," end quote.

Second, continue to provide funding for digital tools and assistance programs in countries where civic space is closed or rapidly closing so that people can access independent sources of information and protect themselves against unwarranted and disproportionate surveillance by their governments.

And, third, pass legislation to improve transparency across technology products and practices in the United States, including content moderation and recommendation systems, as well as the collection and use of data.

It is essential for the United States and other democracies to promote an alternative model to digital authoritarianism through both our foreign and domestic policies.

I will gladly answer any questions you may have. Thank you for having me.

[The statement of Mr. Shahbaz follows:]



PROTECTING A FREE AND OPEN INTERNET

Written Testimony by ADRIAN SHAHBAZ
Vice President, Research and Analysis

Committee on Ways & Means
Subcommittee on Trade

Protecting American Innovation by Establishing and
Enforcing Strong Digital Trade Rules

September 20, 2024, 9:00 a.m.

Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee,

It is an honor to testify before you today. I ask that my full written testimony be admitted into the record.

I am grateful to this subcommittee for elevating the human rights angle of digital trade. The protection of fundamental freedoms is necessary for upholding a rule of law system that protects innovation and enables both prosperity and security. We appreciate Congress' longstanding and bipartisan support for these issues.

I speak today on behalf of Freedom House. We are a nonprofit and nonpartisan organization founded in 1941. Our mission is to protect and expand freedom around the world. My remarks will draw on findings from Freedom House's annual [Freedom on the Net](#) report, which assesses respect for internet freedom in over 70 countries.

Internet freedom is the simple notion that the same rights held by people offline should be protected online. This includes freedom of expression, access to information, and privacy.

We also believe that an open, interoperable, and global internet contributes to the enjoyment and protection of these rights. With the right tools, a schoolteacher in Afghanistan can access the same information and platforms as a student in Washington, D.C. A free and open internet is one that

empowers individuals to learn, communicate, and form communities wherever they are in the world.

For these reasons, [we expressed concerned](#) one year ago when the United States Trade Representative dropped support for cross-border data flows at the World Trade Organization. The decision risks further fragmenting the global internet and emboldening authoritarian governments.

Two-thirds of internet users now reside in countries where political, social, or religious content is censored. More governments have criminalized nonviolent speech and put critics in jail. Increasingly, they seek to divide the global internet into patchwork of national networks that are more easily controlled.

One of the methods used to exert greater control is data localization. These are legal requirements for companies and other service providers to store data about local residents on servers based within the country. They are often passed under the premise of defending national security, growing the digital economy, or protecting users' privacy.

In [our research](#), we have found that these laws can have negative implications for people's freedoms, because they grant a country's security agencies more power to monitor and imprison people who criticize the government or speak up on banned issues. This is particularly true in countries with weak respect for free expression and the rule of law.

One of the clearest examples is China, a one-party state that holds the dubious distinction as the world's worst abuser of freedom. Many US-based news outlets and social media platforms are blocked, including Facebook, WhatsApp, Instagram, YouTube, and X. Those companies that remain in business face data localization requirements and restrictions on cross-border data flows.

Certain providers are required to store personal information about clients and users on local servers, where it is subject to requests from security agencies. Those requests can put companies in a very difficult position – particularly when they are demands to censor legitimate speech, or to help the Chinese Communist Party to gather data about journalists, dissidents, and members of persecuted ethnic and religious communities. According to a [2022 survey by the US-China Business Council](#), these restrictions “disproportionately harm the operations and competitiveness of foreign businesses in China that leverage global infrastructure”.

The Russian government has long admired China's so-called Great Firewall of internet controls. Over time, authorities have passed legislation and developed technical infrastructure to build what they have called a "sovereign internet." Right now, many Russians rely on virtual private networks (VPNs) and other circumvention tools to communicate with family and friends across borders, and to access independent news sources that are based in freer countries. The sovereign internet project would allow Moscow to totally isolate the country from the rest of the internet during mass protests and other major events, cutting off Russians' ability to communicate with the outside world.

As part of this effort, the Russian government has passed a series of law that require companies to collect data on their users, store it on servers based in the country, and hand it over to security agencies like the Federal Security Service (or FSB) when they request it. Companies face demands to comply with unjust censorship and surveillance. Authorities have banned criticism, organizing, and objective reporting on the war in Ukraine. Companies that refuse to comply with the government's demands to enforce their unjust laws are eventually forced to leave the country.

The Chinese and Russian governments are working with other authoritarian leaders to reshape global cyber norms in their interests. At the United Nations and other multilateral fora, they seek to legitimize their domestic crackdowns on freedom and privilege their ability to control data.

If global norms further shift in favor of data localization and restrictions on cross-border data flows, there is a risk that companies in authoritarian countries and backsliding democracies will face increased demands to censor legitimate materials and hand over data about their users. In places where one's political opinions, religious beliefs, and gender or sexuality can be labeled as extremist, these trends may lead to increased persecution of journalists, lawyers, politicians, and ordinary people who speak out against the government.

The United States plays a critically important role in protecting the free flow of information and data across borders – a necessary condition not only for the protection of rights but for the protection of innovation, prosperity, and security. In line with the [United States International Cyberspace and Digital Policy Strategy](#), the US should "develop shared mechanisms that will help maintain an open, interoperable, secure, and reliable internet as well as trusted cross-border data flows." To ensure the United States continues its leadership role in this space, Congress should:

1. Urge the Biden administration and the next presidential administration to ensure the USTR is firmly committed to protecting the free flow of data.
2. Work with the Executive Branch to ensure robust US participation at multilateral institutions. American absence in these spaces makes it easier for authoritarian regimes to push their models of digital authoritarianism internationally.
3. Ensure US trade policy takes a potential trading partner's record on human rights – including protection of a free and open internet – into account.
4. Continue to provide funding for the protection of a free and open internet, including support for local civil society organizations that work on these issues, as well as for popular circumvention tools that allow people in closed environments to access information.
5. Pass legislation to improve transparency across technology products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and political and targeted advertising. Laws should also provide opportunities for vetted researchers to access platform data, in order to inform additional policy development.

It is essential for the US and likeminded allies to offer an alternative to the authoritarian model of digital governance. We should better safeguard people's rights and data while still protecting the global internet.

I will gladly answer any questions you may have. Thank you again for the opportunity to participate in today's briefing.

Chairman SMITH. Thank you, Mr. Shahbaz.
Mr. Gottwald, you are recognized for five minutes.

**STATEMENT OF ERIC GOTTWALD, POLICY SPECIALIST ON
TRADE & ECONOMIC GLOBALIZATION, AFL-CIO**

Mr. GOTTWALD. Good morning, and thank you, Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee, for the opportunity to testify today.

I am here on behalf of the AFL-CIO and the more than 12.5 million union members who work in every State in every sector of our economy.

Too often the digital trade discussion sounds like it has no grounding in the physical world. It is buzz words, like internet-enabled commerce, big data, and cloud computing. It is all those things, but we should not lose sight of the fact that decisions about the abstract things like global data flows, algorithms, and artificial intelligence have profound implication for workers around the world.

While the digital transformation has driven real gains in communications, transportation, science, and beyond, it has brought urgent challenges to the world of work. For example, open global data flows have enabled the offshoring of tens of thousands of good call center and back office jobs to places like India and the Philippines, with low pay and poor working conditions. Major platforms like Facebook and TikTok have outsourced content moderation work to developing nations, where hundreds of thousands of so-called ghost workers spend long days tagging and coding off offensive images and other content.

Digital trade also powers the algorithmic management software that increasingly hires, evaluates, monitors, and even fires workers here in the United States. These technologies can shortchange workers' earnings, expose workers to unsafe work conditions on the job, infringe on the right to form unions, and exacerbate employment discrimination. All these workers are directly impacted by global digital commerce on the job, but they are also impacted at home.

Big tech companies collect, combine, and can modify vast troves of personal data that compromises everyone's security and privacy. Our personal data is sold and resold by unaccountable data brokers to entities in Russia, China, and beyond. Meanwhile, the algorithms that power social media have pushed online hate, political disinformation, and harmed the mental health of young people.

Unfortunately, at a time when we need Congress to regulate the digital economy, the USMCA digital language fits more like a straitjacket than a well-tailored suit. For example, under these rules, governments may not enact any measures that restrict cross-border data flows, with no exception for sensitive forms of personal information. In addition, there is an absolute ban on data localization policies even for legitimate purposes, like ensuring that citizens' sensitive medical or financial information is kept onshore.

Supporters of these severe disciplines point to the agreement's legitimate public policy exception to reassure policymakers that they have retained their full right to regulate. But upon closer examination, this simply isn't the case. The public policy exception is taken

directly from existing WTO agreements where it has proven to be largely ineffective. Just fewer than 5 percent of challenged government policies have been upheld by trade dispute panels.

We are alarmed that bipartisan efforts to protect personal data and address Big Tech's anticompetitive practices could run afoul of these digital trade rules. This debate cannot be framed as a binary choice between China's great firewall and a totally unregulated global data marketplace where anything goes.

It is time for a strategic reset to ensure that our digital trade policy strikes the right balance between promoting open data flows and securing data privacy and workers' rights.

Congress must be free to act to protect Americans' data privacy in advance of our economic and national security interest, even if those measures happen to restrict open global data flows. Congress must preserve the ability of regulators to meaningfully oversee the use of artificial intelligence, management software in the workplace, to ensure that it is consistent with our current labor and employment law. And we must enact new laws to address emerging issues, such as electronic workplace surveillance and the erosion of digital privacy.

The Congress and the public should decide the rules of the road for technology in the workplace and society. That cannot be left up to big tech companies and unaccountable international trade tribunals.

Thank you. I am happy to answer any questions.
[The statement of Mr. Gottwald follows:]

AFL-CIO

**Testimony Before the
Subcommittee on Trade
U.S. House Committee on Ways & Means
118th Congress, Second Session**

**Eric Gottwald
Policy Specialist on Trade and Economic Globalization
AFL-CIO**

**Hearing on “Protecting American Innovation by
Establishing and Enforcing Strong Digital Trade Rules.”**

September 17, 2024

Thank you, Chairman Smith and Ranking Member Blumenauer, for the opportunity to testify before your committee on “Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules.” This testimony is submitted on behalf of the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) and the 12.5 million workers represented by its 60 affiliated unions.

As the Biden administration continues to remake U.S. trade policy, we firmly believe its “worker-centered” approach must extend to digital trade and the digital economy by placing the needs of workers, consumers, and society ahead of the profits and interests of big technology companies. Accordingly, Ambassador Katherine Tai’s decision to re-examine U.S. digital trade policy provides a vital opportunity to strike a better balance between promoting a robust digital economy and other vital public policy objectives.

To date, the digital chapters of recent U.S. trade agreements have prioritized securing increased market access and broad protections against emerging forms of regulation for its big technology firms with broad prohibitions against any government measures that could restrict corporations’ ability to move, process, and store data as they see fit. By comparison, they make no reference to workers’ rights and do not require governments to take any meaningful action to protect individuals’ personal data.

While the digital transformation has driven real gains in communications, transportation, science, and beyond, it has also brought urgent challenges to the world of work and society, which democratic governments are only beginning to address.

Technology companies and other employers are increasingly supervising, surveilling, and even disciplining workers with automated artificial intelligence (AI) and algorithmic management systems that can shortchange workers’ earnings, expose workers to unsafe workplace conditions, infringe on the right to form unions, and exacerbate employment discrimination. Platform companies like ride-hail and delivery services have promoted a new, exploitative model of

employment where so-called “gig” workers endure low earnings, uncertain work schedules, and no benefits. The digital transformation has enabled the corporate offshoring of whole new categories of jobs, including workers in call centers, information technology, back-office, and even health care through telemedicine. It also facilitates the privatization of public data and data services, costing jobs and undermining the quality of publicly delivered services. Many of these jobs are being shipped to countries where workers are paid poverty wages and face severe repression for organizing trade unions.

Outside the workplace, digitalization poses other threats to workers, consumers and people. The large technology companies collect, share, commodify, and sell tremendous amounts of personal data with little or no oversight. Digital apps and social media platforms have eroded personal privacy, undermined the mental health of adolescents, and provided a megaphone to anti-democratic and hateful forces that have corroded the social discourse.

As United States Trade Representative Katherine Tai stated in 2021, digital trade must be “grounded in how it affects our people and our workers” and provide space to “prioritize flexible policies that can adapt to changing circumstances” of rapidly evolving forms of digital commerce.¹ Achieving this vision will require a more balanced approach that preserves the right of governments to fully regulate the digital economy, while also driving greater cooperation to address the very real threats to privacy, democracy, and decent work.

I. Preserving governments’ right to regulate the digital economy

The rapid digital transformation of the economy has emerged largely without the knowledge, consent, or input of the people it most affects — the workers and consumers whose lives are increasingly governed, surveilled, and commodified by the technological revolution.

At a time when governments around the world are grappling with how to regulate emerging digital technologies, recent U.S. digital trade agreements have granted broad digital corporate rights while imposing rigid restrictions on the measures governments can adopt to promote legitimate public policy interests like protecting data privacy, ensuring emerging technologies comply with domestic labor laws, promoting competition, and more. These digital provisions mirror and amplify parallel efforts by Big Tech firms to avoid regulatory oversight in the United States and countries around the world.

The current digital trade model grants broad rights to technology and other companies to control, transmit, process, and store data worldwide, while also shielding their digital systems from regulatory scrutiny. For example, the USMCA and U.S.-Japan digital texts prohibit any restriction on cross-border data flows, with no exception for sensitive forms of personal information. Although the texts contain an exception for “measures necessary to achieve a legitimate public policy objective,” in practice this language — which is borrowed from existing

¹ Tai, Katherine. Ambassador, Office of the U.S. Trade Representative, [“Remarks of Ambassador Katherine Tai on Digital Trade at the Georgetown University Law Center Virtual Conference,”](#) November 3, 2021.

WTO agreements — has been narrowly interpreted by dispute panels and has not proven effective at safeguarding governments’ right to regulate.

The USMCA also contains an absolute prohibition on “data localization” policies, which an increasing number of governments are adopting to require that some kinds of data be stored on domestic servers to protect digital privacy or ensure appropriate access for regulators and law enforcement. Unlike the prohibition on restrictions to cross-border data flows, it contains no “legitimate public policy” exception.

In addition, the USMCA adopts a broad prohibition on government access to or forced transfer of corporate source codes and algorithms as a condition for allowing the sale and distribution of digital products in a given country. While the text allows for disclosure on a case-by-case basis to a regulatory body or judicial authority, this is limited to a “specific investigation,” which could preclude broader, industry-wide investigations necessary to address the harmful impact of algorithms, artificial intelligence, and machine learning on workers and people. The specific investigation clause also leaves it unclear how governments could initiate an investigation into, for example, employment discrimination and AI management software, without first having the broad authority to conduct an initial review of source codes to understand how they function and what their impacts are in the workplace.

The sweeping nature of these commitments is alarming given that most countries, including the United States, lack a comprehensive federal regulatory framework to address the downsides of digitalization on workers and society. The “legitimate public policy objective” exception lifted from the WTO has proven difficult for countries to invoke in practice, even with regard to sectors with long-standing, well-established regulatory regimes. Applying these restrictions to the fast evolving digital economy risks locking in an unregulated status quo that only benefits large technology companies and could undermine efforts to safeguard worker and consumer data privacy.

The rapidly evolving digital economy warrants new approaches to address the negative impacts of digitalization on workers, consumers, and society. The absence of domestic measures governing the digital economy heightens the importance that digital trade agreements must preserve robust public policy space. A worker-centered digital trade agenda must enshrine the right-to-regulate these new technologies to protect workers and consumers by enforcing current law and addressing emerging impacts on the workplace and society.

II. Advancing a pro-active agenda to safeguard workers’ rights, protect data privacy and security, and combat low-road digital offshoring.

In addition to preserving policy space to regulate, a worker-centered digital trade policy should also include positive commitments by governments to address the myriad of challenges connected to the digital transformation. Commitments to promote reliable, secure cross-border data flows must be offset by corresponding obligations to properly regulate the digital economy, including by addressing a range of issues that threaten workers’ rights and privacy in and out of the workplace:

- **Ensure that digital trade agreements are subject to strong and enforceable labor standards:** Given the growing importance of the digital economy, it is essential that countries establish strong guardrails to avoid a race to the bottom in regulation and corporate conduct. Digital trade agreements must contain an obligation to respect the internationally recognized workers' rights contained in the 1998 International Labor Organization Declaration on Fundamental Rights and Principles at Work. In addition, they must contain strong monitoring and enforcement mechanisms to ensure government and corporate compliance.
- **Require governments to enact strong policies to safeguard individuals' personal data:** Governments should be able to adopt restrictions on cross-border data flows to protect the privacy and security of individuals' personal data. In our hyper-connected online world, consumers and workers' personal data is increasingly monitored, collected, shared, analyzed, and sold by companies without their knowledge, consent or oversight. The existing digital trade model promotes a voluntary form of corporate self-regulation that has proven inadequate to protect individuals' personal information. Digital trade policy should encourage rather than deter government efforts to safeguard individuals' personal data inside and outside the workplace.
- **Authorize governments to enact data localization policies with regard to certain categories of sensitive data:** While open data flows are essential to the modern global economy, not all data is the same. Governments should have the ability to require that individuals' sensitive personal information (medical, financial, and biometric data collected in the workplace) or data related to certain sectors (critical infrastructure, national security, law enforcement) be kept onshore to ensure it is subject to strong and enforceable privacy standards and effective government oversight.
- **Discourage low-road digital offshoring:** Safeguarding critical, vulnerable, and personal data not only protects the security of people and the economy, but it also helps keep good jobs here in the United States. Big Tech companies and other employers have demanded unfettered cross-border data flows, in part, to facilitate the offshoring of digitally enabled back office, call-center, data processing, telemedicine and other jobs. Many of these jobs are going to countries with weak data protection regimes and widespread labor rights abuses. For example, tens of thousands of Communications Workers of America (CWA) members have lost call center jobs due to digital offshoring to countries like Mexico and the Philippines.² Digital trade agreements should actively discourage this type of low-road offshoring that lowers labor standards, while also placing customers' data at greater risk.
- **Facilitate meaningful oversight of source codes and algorithms to ensure compliance with labor and employment laws:** Employers are increasingly using automated, algorithmic systems to hire, manage, control, monitor, discipline, and even fire workers

² Sainato, Michael. "They're liquidating us': AT&T continues layoffs and outsourcing despite profits." The Guardian. August 18, 2018

largely without the knowledge, consent or input of workers or unions. These new employer tools can undermine workers' rights, compromise workplace safety, violate wage and hour laws, and discriminate against protected classes of workers in hiring, promotion, or termination. Women, people of color, and immigrants are particularly at-risk, as they are more likely to be employed in lower-wage workplaces where these technologies are widely deployed.

Millions of workers in the United States already face challenges from algorithmic management. Amazon's algorithmic warehouse productivity software has created inhumane working conditions where workers are punished for taking bathroom breaks and suffer far higher serious injury rates. Some school districts have been using algorithmic tools to evaluate teachers based on how students perform on tests and to discipline and even fire teachers whose students failed to measure up to a computer modeled test score target. Automated monitoring of call center workers can incorrectly punish agents for allegedly straying from their scripts because the speech recognition software can discriminate against workers with accents, dialects, or different speech tones. In the retail and food service sectors, employers are increasingly using algorithmic "just-in-time" scheduling software that has led to erratic working schedules, unpredictable pay, and threatened health care benefits.

A worker-centered digital trade agenda must ensure that companies are held accountable for the risks associated with automated systems that implement critical decision-making protocol. It should be mandatory for companies to disclose to governments the impact assessments of their automated systems to ensure they are compliant with existing labor and employment laws. In addition, it should facilitate intergovernmental cooperation to address the risk that AI management software is undermining worker safety, wage and hour laws, and anti-discrimination laws.

- **Address emerging threats to workers' privacy, including employer use of workplace surveillance software:** Employer use of digital workplace surveillance tools has skyrocketed during the pandemic with the rise of telework. Workers have little protection from digital workplace surveillance including vehicle telemetry, hand-held equipment that evaluates work speed, keystroke and camera monitoring, and even surveillance of workers' social media presence to assess union sympathies. Employer use of these tools can contribute to workplace safety problems, lead to anti-union coercion and retaliation, and erode worker privacy. A worker-centered trade agenda should require governments to adopt measures to address digital workplace surveillance and other emerging threats to workers' privacy. For example, employers should be required to disclose their use of surveillance tools, what kind of data is collected and for what purpose, whether the data is sold to or shared with third parties, and provide a right for the employee to review and correct any inaccuracies.
- **Address abusive employment practices in the technology sector:** Large technology and platform companies like Uber and Facebook have promoted an exploitative employment model based on rampant employment misclassification and the outsourcing

of core job functions. Hidden behind social media platforms and popular digital assistants like Siri or Alexa are an army of outsourced “ghost workers” who code and enter data, transcribe digital assistant audio recordings, and monitor online platforms for violent and offensive content. These workers, many of whom work in developing countries, are essential to training AI algorithms and keeping hateful and offensive content off social media platforms. Platform gig workers and the ghost workers that power AI systems are employed as precarious contractors with no benefits, sick leave, guaranteed minimum wages, or the ability to form unions and bargain collectively. A worker-centered digital trade approach would require big technology companies to eliminate the labor abuses in their own operations and supply chains.

- **Protect and promote the economic security of creative professionals in the U.S.:** A worker-centered approach to digital trade must protect and promote the economic security of the more than 5 million people who work in the motion picture, television, music, and other parts of the creative sector. Many of these workers earn collectively bargained pay and contributions to their health insurance and pension plans from the sales and licensing of the copyrighted works that they help create. Digital trade policy must aggressively address the stolen or unlicensed use of copyrighted content on digital platforms and avoid replicating the outdated, overbroad copyright safe harbor exclusions that exist in some U.S. laws. In addition, it should promote the “no collection without distribution” principle to address the unfair practice by some countries of collecting royalties based on the work of U.S. creative professionals without passing it on to the artists, depriving them of rightful compensation for the use of their work.
- **Stop the misappropriation of voices, images, and likenesses for use in AI-generated digital content:** It is already clear that there are the dangers and downsides to AI, including image-based sexual abuse, misappropriation for commercial gain, and the proliferation of “deepfake” videos where the digital likeness of one person – usually a celebrity – is transposed onto another the body of another individual without their consent. Digital trade policy must ensure that there are safeguards against these abuses, while also holding online platforms accountable for unlawful user content they themselves facilitated or profit from.
- **Address the rise of cybercrime by both state and private actors:** In 2014, the U.S. charged several Chinese military members with hacking multiple U.S.-based companies and the United Steelworkers. In 2019, the International Brotherhood of Teamsters (IBT) experienced a ransomware attack demanding \$2.9 million that forced the union to rebuild computer servers. Digital trade policy must strive to improve cyber security and create a common enforcement agenda to hold the criminals and companies that facilitate these crimes accountable.

III. Conclusion

Too often, the debate over digital trade is unhelpfully framed as a binary choice between authoritarian digital censorship or the unregulated status quo where companies are largely free to collect, analyze, process, and sell workers and consumers' private data as they see fit. The labor movement rejects this false choice and instead calls for a new democratic, stakeholder-driven approach to data governance that addresses the negative impacts of digitalization on workers, consumers, and society.

To date, U.S. "digital trade" agreements have sought to expand market access for large technology companies by granting broad digital data and IP rights while narrowly constraining the ability of governments (both the United States and our trade partners) to adopt measures to address the digital economic transformation. This combination of broad corporate rights and limited domestic governance threatens to lock-in the current unregulated digital environment that poses significant risks to workers and society.

The Biden administration's worker-centered trade policy is a major opportunity to correct for this narrow, corporate approach to allow for broader policy space to protect personal data, strengthen economic security, protect domestic jobs, and tackle the downsides of the digital transition on workers, consumers, and society. As democracies seek to create a digital economy that is fair and inclusive, digital trade policy must also evolve to facilitate new forms of domestic and international regulation and oversight of the digital economy.

Chairman SMITH. Thank you. Thank you, Mr. Gottwald.

Thank you to our entire panel. I think we have a great variety of perspectives here that I think are important to include. It cannot be overstated how important this topic is. So thank you for sharing your perspectives and your insight.

I think one of the coolest things about digital issues, digital technology is that it has been, I think, a great equalizer in so many different ways. We see technology perhaps the backbone from a larger company, but it is a launching pad for a small operation.

So, Dr. Walch, I don't know how many employees you have, but I am guessing you started out smaller than you are now, and that many, many other companies have as well.

I might say that, you know, American digital services or digital services that originate in our country allow—you know, they provide a launching pad for other small operations around the world too. So it is discouraging that other countries, other jurisdictions would even want to restrict that when perhaps they are conceivably harming their own population.

But getting more specific here, I know that two years ago, we as a country engaged with Kenya—well, actually before that as well—launching negotiations for what is called the Strategic Trade and Investment Partnership. So at that time, USTR highlighted digital trade as a key priority in the negotiations. However, digital trade has kind of dropped off of that discussion. I find that particularly concerning.

But, Dr. Atkinson and Mr. Shahbaz, what would you say about what I would think is a missed opportunity here, especially when you look at opportunities across the continent of Africa and the capacity that they can bring to the entire arena of international trade? And I am just wondering if you could share your perspective on that.

Mr. ATKINSON. Thank you. The ITI has just released a big report up here in the Capitol on Wednesday looking at how innovative Chinese firms are and what the competition we face with China. And one of the main battlegrounds for that competition, including in the digital space, is going to be in places like Africa, South America, parts of Asia. And so I think we have to think about Africa as a battleground. This is similar to how we thought about it in the Cold War. We were vigilant to make sure that African countries didn't go and side with the Soviets.

So by walking away from digital trade engagement, I think we are opening the door to the Chinese. They are spending billions and billions of dollars in African countries to get them to adopt the kinds of systems we heard about, the surveillance systems and others. So if we don't engage with countries like Kenya, I really worry that they are just going to default to a country like China that is much more enabling and supportive of what they are doing.

Chairman SMITH. Thank you.

Mr. Shahbaz.

Mr. SHAHBAZ. Thank you for the question.

I would say, you know, Africa is an incredibly diverse continent, and you have democracies and autocracies there. I would echo what Dr. Atkinson said here that when we have interviewed several experts and those who are engaged in the fight for freedom and for

digital freedoms on the continent, what they have shared is their fear, essentially, around data localization laws; that if more governments are passing data localization laws, that will put their very sensitive information closer to the hands of security agencies. And this information reveals one's political opinions, one's religious beliefs, also sensitive information about our health, our connections, and it is essentially a threat to privacy.

So what we have wanted to see happen is for the United States to offer an alternative to the digital authoritarian model that the Chinese Government has been promoting on the continent. They have been undergoing trainings and investments throughout the continent.

I think it is important that the United States' approach, not only favors the free flow of information and data, but then also worked with civil society and with government to make sure that the operating system of democratic governance is actually there in place, to make sure that whatever rules or technologies that are then brought in in these countries is essentially under the oversight of the people. Because we essentially believe that democracy is the most important technology here and many of these societies need in order to make sure that technology is used to promote freedoms.

Thank you.

Chairman SMITH. Thank you.

Dr. Atkinson, I know that there has been criticism of strong digital trade rules saying that there is a concern about the right to regulate, perhaps—for our country to regulate.

Do you think that there are any provisions in our trade agreements that would prevent Congress from passing new legislation on topics such as artificial intelligence or data privacy?

Mr. ATKINSON. There absolutely are not. I would disagree with what Mr. Gottwald said. He mentioned, for example, open data flows lead to offshoring. That is about U.S. policy. That is not—if we want to just not do that, we could.

Digital trade leads to employee oversight. No. Employee oversight, which oftentimes is a good thing, is about a domestic issue. If you want to regulate how technologies monitor their employee, you have every right to do that. It is not going to violate any trade agreement.

Privacy. You know, I go back to this key point. We can and should have a national privacy bill, but it doesn't mean that a company doing business here can't move the data to a server or a cloud center in Ottawa or in Montreal. There is nothing that makes that—that impedes what you want to do.

The only thing that would impede what you want to do is if you decide you wanted to—if Congress wants to put in place laws that intentionally discriminate against foreign companies. That is what you cannot do. That is the tie that binds, if you will.

So, no, Congress could easily pass AI rules, as long as the AI rules and regulations don't discriminate against foreign AI companies in favor of American AI companies. But if you want to pass a law that says that AI has to have special privacy rules, or that algorithms have to be disclosed, or whatever you might want to do, you can do that.

Chairman SMITH. Thank you.

I will now move to Mr. Blumenauer as ranking member for his questions.

Mr. BLUMENAUER. Thank you, Mr. Chairman.

Mr. Shahbaz, in your testimony, you say it is essential for the United States and like-minded allies to offer an alternative to the authoritarian model of digital governance. We should better safeguard people's rights and data while still protecting the global internet. And you identify a half dozen specifics.

Can you elaborate on what the one or two priorities would be to be able to accomplish that objective?

Mr. SHAHBAZ. Thank you. It is a great question, and I think is it one where the United States has made progress over the past several administrations.

So I would just point to the longstanding bipartisan support for global internet freedom programs, which have really made a difference throughout the African continent, as well as around the world, to provide people with greater access to information.

Congress funds programs that provide virtual private networks and other types of circumvention tools that allow for people in closed environments to, let's say, jump the censorship of their local government and prevent their activity from being under close surveillance. So I would say that promoting circumvention tools is one aspect of that.

A second part is what I alluded to, which is a more democratic model for digital governance. So what we are seeing around the world is that China, Russia, Iran, other authoritarian governments, are privileging a state-centric view of how the internet should be run. And that goes against the fundamental multi-stakeholder model of internet governance.

There are conversations that are happening right now as we speak around internet governance. There is a U.N. cyber crime treaty that is deeply troubling. It has certain provisions that are deeply troubling that would allow for authoritarian governments to collaborate by sharing data about people who are suspected of crimes in their countries. So there is quite a bit that the United States should also be doing multilaterally.

I would say a fundamental point here is really the support for civil society. Because what distinguishes democracy, and what the United States is doing from what China is doing, is working not only with governments or with security agencies to protect countries and protect national security, but it is also working with civil society organizations in a lot of these countries to make sure that they have a voice at the table. And we have seen that pay dividends.

When many countries have introduced legislation for data localization requirements, it has been actually civil society organizations that have been at the table, raising a ruckus locally, through the media, through conversations with legislators there, to then push back against very far-reaching laws that would essentially cut the countries off from the rest of the global internet.

Thank you.

Mr. BLUMENAUER. No, thank you.

Mr. Gottwald, in your testimony, you noted that employers are increasingly using automative systems to monitor or discipline

workers, largely without the input of workers or their unions. I hope we could get a little more granular in terms of what this means and how we can speak out and take action to protect the rights of workers.

We took a CODEL to Colombia looking at the implementation of our FTA in dealing with call centers. It seemed to me that there are some gaps here that we might be able to do something with. Would you elaborate on your point?

Mr. GOTTWALD. Thanks for that question.

If we step back, I think everybody has recognized, since the pandemic hit and telework became more and more popular, there is a lot more awareness about the deployment by employers of, you know, these digital workplace surveillance tools. Some of these are quite creepy, to be candid with you.

If you are working from home and your employer is monitoring not just key strokes but potentially even using the camera to biometrics and things, and it is very—it is a little disturbing. So I can understand why Congress is focused on this. Utterly appropriate.

I will just say that, in our experience, workers are almost never aware that this software is being deployed by the employer. Sometimes the trade unions, if there is a trade union, are unaware of it as well. Although I will say this: Our trade unions are more and more making this subject of use of AI management software or surveillance software part of collective bargaining. And I think that is a very positive trend. I think that, you know, it influences the workplace so profoundly. And workers need to know what kind of data is being collected by the employer and what is being done with that data. Is it being sold and shared, resold? I mean, there is a lot to unpack here.

I am glad you mentioned the call center workers. They face special challenges. We have heard from call center—organized call center workers that employers sometimes use this monitoring soft—quality monitoring software, which is fine. But what will happen in practice is it will punish people with non-English—non-native English speakers. They speak English well enough, but their accent—they might have a slight accent this way or that way—and they are probably well understood by the person on the other side of the line, but the software is, you know, knocking them for, you know, for having an accent that is a little bit outside the box.

Mr. BLUMENAUER. Thank you.

Mr. GOTTWALD. The last thing I would say is, in Colombia, that company, I believe you—was Teleperformance, large French company that does a lot of outsourcing work for call centers for the Big Tech companies. That Teleperformance company has a horrible track record on workers' rights. A complaint was filed by French unions at the OECD really laying out the challenges in this area.

And, Mr. Blumenauer, I can follow up in written remarks to give more flavor there.

Mr. BLUMENAUER. I would appreciate that.

Thank you, Mr. Chairman.

Chairman SMITH. Thank you.

I will now move to Mr. LaHood, followed by Mr. Kildee. After Mr. Kildee, we will move, as is tradition, two to one for the questions.

Mr. LaHood, you are recognized for five minutes.

Mr. LAHOOD. Thank you, Mr. Chairman. And thank you for having this important hearing today.

I want to thank all of our witnesses for your really valuable testimony here today on a very important topic.

In our increasingly interconnected world, the trade of digital goods and services is essential for American growth, innovation, and global leadership. Digital trade is more than buying and selling of goods online. It encompasses a global flow of data, ideas, and talent.

In 2022, digital trade encompassed more than \$2.5 trillion of U.S. economic activity, and represents the fastest growing segment of global trade.

As the co-chair of the Digital Trade Caucus here in Congress, I am increasingly concerned about the proliferation of restrictive and oftentimes discriminatory digital regulatory frameworks and laws which risk curtailing American digital competitiveness.

In recent years, we have seen close trading partners, including Canada, Australia, Korea, and the EU, enact regulatory frameworks or levy digital service taxes that risk unfair treatment of American businesses.

While laws like the EU's Digital Marketing Act, the DMA, or Digital Services Act, DSA, are intended to create fairer digital landscape and simulate domestic competition, in practice, they often discriminate against U.S. companies, posing challenges that stifle innovation and competition.

I think it is also important to remember the U.S. leads the world in technology. We lead the world in digital competition. We need to be much more aware of that when we look at what Europe and a number of other countries are doing.

In 2023, the European Commission identified six gatekeeper platforms to be subject to regulation under the DMA or face fines equating to more than 10 percent of their global revenues. Of those six companies, five are American and one is Chinese. Isn't that ironic that none of the ones that are headquartered in Europe were a part of that.

In my view, efforts to regulate these American companies can and will lead to a chilling effect, discouraging further U.S. investment in Europe. In fact, a newly released report from the European Commission on the future of EU competition notes that the complexity and risks associated with the EU's regulatory approach may undermine developments in emerging technologies like AI and quantum computing.

Further, I and many others have been critical of the Biden administration's failure to promote a strong alternative that advances American digital trade interest abroad with our like-minded allies and trading partners. Instead, this administration continues to send mixed messages by walking back long-held bipartisan and really nonpartisan digital trade proposals as outlined by the WTO, pushing a narrative that encourages these discriminatory digital frameworks to flourish. And that is troubling.

I will get to my question here. Dr. Atkinson, given the ongoing regulatory approach by the EU, is it possible to find common ground with our counterparts in Europe in terms of digital trade?

If so, what tools should Congress consider to address these regulatory challenges?

Mr. ATKINSON. Well, Congressman, you alluded to what is known now as the Draghi report that just came out, former President of Italy. Very important report because, for the first time, there is a high level of recognition that Europe is shooting itself in the foot with these policies. So whether that really changes or not, I don't know.

I am very skeptical that we can get agreement or even close the gap with the Europeans, absent being tough. I think the Europeans understand they can get away with this, and they have been getting away with it constantly. And there has been no pushback, there has been no penalties. In fact, we have engaged with the tech and trade council and had these conversations. There is no penalties.

So I think the Europeans, as a rational actor, would say, yeah, why not. Let's keep punishing American companies. Let's keep taking their money. I mean, they can fund the—I am kind of exaggerating—they can fund the European Commission budget just off the fines of American companies.

So I think the only way to do that is to say there will be consequences if you keep doing this. We could bring a 301 case, for example. We could penalize them on other areas. I lay that out in my testimony. So I think absent getting tough, they are just not going to respond.

Mr. LAHOOD. The bottom line is we have many tools in the toolbox to put deterrence in place and hold the Europeans accountable. Is that fair.

Mr. ATKINSON. We have many tools in the toolbox. We could add a few more. Yes, that is absolutely—that is absolutely—I would agree with that.

Mr. LAHOOD. Thank you. I yield back.

Chairman SMITH. Thank you.

I now recognize Mr. Kildee from Michigan.

Mr. KILDEE. Thank you, Chairman Smith and Ranking Member Blumenauer. And especially thanks to the witnesses for being here for this really important conversation.

Many of us on this committee, and the Biden-Harris Administration, by the way, have been committed to creating a fair playing field for American workers to compete in the global and increasingly digital economy.

One way to help workers stay competitive, of course, is by ensuring that U.S. international trade agreements specifically uphold workers' rights. Our agreements that cover digital trade should not be any different. We need strong, enforceable labor standards in these agreements to avoid the inevitable race to the bottom when it comes to the treatment of workers.

This could mean enshrining internationally recognized worker rights by outlining the ILO's declaration of fundamental rights and principles that work, as well and importantly, creating, monitoring in enforcement mechanisms as we have seen in other trade agreements.

So, Mr. Gottwald, coming back to you, and you have made mention of some of this both in your written testimony and in answers

to questions here. But I wonder if you could elaborate a bit on what these labor standards that I suggest and others have might look like. And if you have examples, model examples of such standards that might already exist. Could you comment?

Mr. GOTTWALD. Thank you, Representative Kildee. Yeah, this is a great question. If we look at the digital economy, it was mentioned before, it is now—you know, it sort of bled into the normal comment—the line is not clear what is digital and what is not anymore. I think everybody knows that.

So if we look at the U.S.-Japan agreement, for example, that was a standalone digital agreement. The problem from our point of view is that, if you look at the text, there is—nowhere in the text does it say “worker,” “labor rights,” anything, because it is a standalone deal.

So I think certainly for these standalone deals, USTR needs to develop some clear labor standards and benchmarks. Much of that, as you mentioned, can be borrowed from our existing trade deals.

Mr. KILDEE. Right.

Mr. GOTTWALD. And based on these 1998 ILO fundamental principles and rights, right? And these principles and rights, by the way, this is the baseline, right? This is the baseline of respect for workers. No child labor, no forced labor. The right to organize a union, right to be free from discrimination at work. I mean, these are the rules that everybody has already agreed to play by at the ILO. So totally appropriate to put those in there and have all the parties to these digital trade deals agree that they are going to uphold these rules, including with workers from the digital sector and the services sector, that is really critical.

I would also say that, to your point on monitoring enforcement, I think we need to get a little more creative on monitoring enforcement for the services sector and the digital trade sector. USMCA with the Rapid Response Mechanism, hugely forward, tremendously effective for targeting employers and facilities who are benefiting from USMCA shipping goods across the border. A bit more challenging with services in digital.

Mr. KILDEE. Right.

Mr. GOTTWALD. Right. Because it is not—sometimes it is not goods going across the border, it is data. So—but smart people over at USTR, smart people in Congress, we can figure it out. And I appreciate you raising it.

Mr. KILDEE. Well, thank you for that.

I wonder if I could just quickly turn to the issue of digital services taxes. We know that there was a discriminatory DST implemented by Canada in June.

Mr. Atkinson, I ask you to comment. Congressman Estes and I have been working together on this, condemning foreign DSTs and how they harm businesses. And you mentioned a couple of times that there are ways we can push back. And I wonder if you might just specifically suggest some ideas that you might have as to how to do that. I mean, obviously, you mentioned, relative to other circumstances, the use of 301.

Do you have ideas on specific ways, other than just raising the issue, specific techniques or mechanisms that we might be able to

use to push back, particularly in this issue that we are having with Canada?

Mr. ATKINSON. Thank you. No, that is the key issue, particularly because Canada's tax is retroactive. So they are going to try to get as much money out of that as possible.

I wouldn't—I think Canada to me is different than Europe, because I think we have a lot more leverage. I think the Cana—I am born in Canada. I am a dual citizen, and—

Mr. KILDEE [continuing]. On the border, they are friends, but we do have our issues.

Mr. ATKINSON. They know more about our politics than I think we do sometimes.

Mr. KILDEE. I think that is true.

Mr. ATKINSON. Very sensitive to being friends with us. So I think we have a lot of leverage if we were strong in pushing back and there was, you know, a leader-to-leader meeting and saying, no, if you do that, we can't.

If that doesn't work, I mean, one of the ideas that we—I laid out in the testimony is an idea from Gary Hufbauer, I think at the Peterson Institute, which would be to pass a law that would allow us to tax their companies in the same way. I guarantee if we were to do that, we would get their attention immediately. They think they can get a free lunch out of this with no penalties to their own companies. Whereas, I think if we said you do that, we are going to tax a bunch of your companies that are doing business in the U.S.

Mr. KILDEE. Thank you, Doctor. I really appreciate the testimony.

I yield back.

Chairman SMITH. Thank you.

I now recognize, from Kansas, Mr. Estes.

Mr. ESTES. Thank you, Mr. Chairman. And thank you to all our witness for being here today.

You know, a week ago, I led our U.S. Innovation Tax Team to a listening tour of what some people call Silicon Valley, others call Tech Valley, in California. While our focus was on encouraging innovation through sound stable tax policies, it didn't take long for the discussions to also include intellectual property, the theft of intellectual property, and extraterritorial foreign taxes.

Bad policies like the TRIPS waiver enforced tech transfers, disincentivized small startups and major corporations from innovating, testing, and developing, and manufacturing here in the United States. And they counter the good policies that we could restore or strengthen, like immediate research and development expensing in the foreign-derived intangible income or FDII.

The TRIPS waiver has put us on a slippery slope. We now have countries at the WTO proposing more forced tech transfers, localized operations, and data localizations, in short, the complete abandonment of U.S. digital trade priorities.

As one startup told me, it is easy to get a shop set up or to move research and development to another country that has more favorable policies, as opposed to punitive ones, and that is not good for our country.

Policies that hurt innovation hurt all Americans because they slow the economy, reduce jobs, and give foreign adversaries a competitive advantage.

Another major area of concern, as we talked about before, is the digital services taxes, or DSTs. We have witnessed countries like France and Canada specifically target U.S. companies to fill their coffers with these disastrous extraterritorial taxes.

One company I talked to used the phrase, “it is a bold grab of U.S. money,” and it is costing Americans billions of dollars.

Dr. Atkinson, OECD’s Pillar One was supposed to provide clarity and stability around DSTs, but instead the Biden-Harris negotiators put America last, and as we have talked about earlier, DSTs are proliferating.

How do we—I know Mr. Kildee had asked some about other provisions we could do, but are there some equitable offsets to discourage foreign countries from thinking they can get away with transferring U.S. dollars? When you mention taxes, are there other things we could do as well?

Mr. ATKINSON. Thank you. This is—I think the first thing to recognize is that pillar one is basically institutionalizing DSTs. That is all it is. Pillar one says you can do a DST; you just have to do it according to these rules. If your profit rate is above ten percent, we get to tax 25 percent of those profits, but only for certain-sized companies even if you—so I think the U.S. administration and Congress needs to come out and say, no, there is no logic behind pillar one.

OECD says the logic behind pillar one is because now we are trading things across borders that we didn’t trade before in services. Well, by that logic, we should have—we should be taxing any company that sells anything in the U.S., even though they don’t have an operation here.

So I don’t know. Maybe there is some French water that comes across the border. Well, we should tax Perrier. I mean, there is no logic behind why you would single out digital.

So I think—I think, again, we have to do two things. One is I like that idea of mirror taxes. Fine, you are going to do that; we are going to tax you—we are going to tax you just as much, if not more. We need to make it clear that they can’t take U.S. taxpayer money.

I think the second thing would be there is a whole set of things we can do around—around trade enforcement that we should say, fine, you are going to do that, we will do this. And I think at the end of the day, it is just a power play. We have to show that we are not going to let them take—take our money.

Mr. ESTES. Mr. Shahbaz, for years we have had major concerns about CCP stealing intellectual properties. As we have talked about advancing technologies such as AI, are you concerned about China and that they continue to ransack our intellectual property and why it is important for tech like this to be fostered in the United States instead of China?

Mr. SHAHBAZ. Thank you for the question. We are concerned about generally the Chinese Communist Party and the government’s influence here in the United States, the ways that it conducts espionage, transnational repression, as well as malign polit-

ical influence. That is where we think it is incredibly important to do two things.

One is to stand up laws that protect—essentially, promote resilience here in the United States, resilience for companies, resilience for individuals who may face attacks from—from the Chinese government and its affiliates. We also do think that it is incredibly important to show why technologies that are developed in the United States and why the United States governance system is very different to that in China.

I think that is an incredibly important message that also sells well to our partners in our countries around the world, those in other markets that are looking to goods. They want to understand why it is that they should be purchasing U.S. technologies rather than those that are manufactured in China.

Obviously, there are some economic considerations where perhaps they may be going for the technology that is the cheapest. But I think that is where the United States can play on its competitive advantage as a democracy, to show that, well, listen, our technology isn't stealing your data. It is not—you know, when there is a smart city that is built by Huawei in Africa or other technologies where Chinese companies are developing the infrastructure, there have been reports that that data is being slowly trickled back to China so that it can be used for Chinese intelligence purposes or for corporate espionage.

So I think it is very important for U.S. companies to show that, you know, that is not part of the game. You know, what differentiates U.S. companies—and this is what I am arguing that we should be promoting—is that we are going to be safeguarding your data. You know, this data is going to be under the oversight of—you know, of the strictest cybersecurity safeguards.

That, I think, is how we differentiate ourselves from the Chinese Communist Party. Thank you.

Mr. ESTES. Thank you. And I want to thank all the witnesses. I know there is a lot more I would like to discuss, but just to close out, I do think that government, both in Congress and the administration, needs to actively defend U.S. innovators and job creators against these assaults.

I yield back, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Estes. I now recognize Mrs. Miller from West Virginia.

Mrs. MILLER. Thank you, Chairman Smith and Ranking Member Blumenauer. And thank you all for being here today to talk about this important issue.

I have already heard several of our close allies mention, specifically Korea, they may soon pass online platform laws and regulations that would make it difficult for our U.S. companies to operate in their country. And I am very concerned that such an important strategic ally like the Republic of Korea is pursuing economic policies that target and discriminate against U.S. technology companies while welcoming state-owned Chinese companies with open arms.

Chinese firms are the fastest growing tech companies in Korea with many leveraging strategic partnerships with Korean monopolies who have a strong influence in Korea's legislature. And as a

result, there are proposed bills and regulations that would inadvertently grant Chinese players an advantage over U.S. firms, supercharging the growth of China's own national champions in Korea.

The U.S. is holding up our end of the technology alliance by providing Korean companies billions of U.S. taxpayer funds in the form of chips grants and EV and battery subsidies. I just kind of find it really concerning that the Korean government is, in turn, treating American interests in this manner, and I am concerned about the national security implication of the ill-advised economic discrimination and would urge them not to go down this path, but, instead, continue our important technology partnership and the goals that are established in our free trade agreement.

Our trade agreement with Korea is the second largest free trade agreement by trade flows second only to the USMCA. It is extremely concerning to me that our two biggest FTAs are both facing obstacles in the world of digital trade.

And I am planning to introduce legislation that focuses on the strength and importance of the United States and the Republic of Korean alliance with the intention to stop the Korean government from implementing these blatantly discriminatory laws that will cause an unnecessary irritant to such a vital relationship, and I do look forward to working with the committee to pass this type of important legislation.

Dr. Atkinson, would you please explain how China wins should Korea pursue economic discrimination policies against the United States, and why are Chinese firms seeking to drastically increase their Korean user base, and do you believe that Korea is assisting them in their growth?

Mr. ATKINSON. Thank you, Congresswoman. One of the key things about Korea, I was just—I spent a lot of time in Korea. They invite me over to talk and the like.

And the last time I was over there with my family, I tried to use Google maps to figure out where to go, and I can't. I could use a Korean app company, which actually I had to do; I had to download. And they say it is national security.

It has nothing to do with national security. It is the fact that they wanted to favor their own domestic map companies, their own domestic players. That is what they are doing now by copying the European DMA.

And what they want to do is they want to be able to pass a law that would require American companies to turn over data to be interoperable to do other kinds of things that would benefit Korean companies, but they can't write the laws so blatantly that admits that. So it would benefit Korean companies, but it would also benefit Chinese companies.

And so they are willing to make that tradeoff because they think it is going to benefit their companies more. It will hurt our companies. So it is almost like—it is almost like, you know, getting attacked not directly. So they are not trying to benefit Chinese companies. They are trying to benefit Korean companies.

But you are absolutely right, this will benefit Chinese companies and make them stronger. I would put Korea, again, in the same

category as I put Canada. They need us a lot more than we need them.

They are dependent upon us, not just for military, but they are so focused right now on building technology partnerships—I just spoke at two conferences here that the Korean government put on. They want technology partnerships with us. And we are going ahead and saying yes, but I think there has to be a quid pro quo with that.

Yeah, we want technology partnerships with you so we can both be stronger against the Chinese, but we are not going to do partnerships with you if you do these kinds of discriminatory things.

Mrs. MILLER. What are the national security concerns related to U.S. foreign policy in the Indo-Pacific? Should the U.S. be less economically tied to our strategic ally as they grow closer to China?

Mr. ATKINSON. So the fundamental question, I think, in the Indo-Pacific is, are these countries going to gradually move over into the China orbit, or are they going to stay in the Western Democratic market orbit. And that is—we are going to know that in 20 years. That will be decided.

And by letting the Koreans, sort of, have it both ways—the Koreans don't want to pick. They want to have really close relationships with the Chinese because they know Chinese are predatory and retaliatory. They will hurt the Korean companies. They have done that before.

But we need to let them know that they can't have it both ways. They have to pick. We are their defender. They need to be on the side of the allies and democracy. So I think it is a critical, critical issue that we make them choose and choose us.

Mrs. MILLER. Thank you. I guess I need to yield back my time. I am not finished, though. Thank you.

Chairman SMITH. We will try to circle back around if we can. I now recognize Ms. DelBene for five minutes.

Ms. DELBENE. Thank you, Mr. Chairman, and thanks to all our witnesses for being here. This is a really important conversation.

Ever since I arrived in Congress, I have been advocating for a federal consumer data privacy law. Every day millions of Americans' personal information is at risk, and we have to put people back in control of their data. And this has been crystal clear in debates around reproductive health data, TikTok, AI, and on and on and on.

Ambassador Tai has maintained that one of the reasons that the U.S. has paused digital trade talks is that they may limit the policy space needed to address domestic policy issues, like privacy. Her argument is that, by entering into digital trade agreements, the U.S. is giving up its ability to regulate domestically.

That said, if we step back from the negotiating table until Congress acts, we run a serious risk of harming the very objectives, such as defending American companies, protecting privacy, and supporting a free and open internet, that have been core to U.S. policy for many years.

So, Mr. Razis, I guess I will start with you. Does the U.S. entering into trade agreements prevent Congress or the administration from legislating or regulating on important issues domestically?

Mr. RAZIS. Thank you for the question, Congresswoman.

In short, no. We don't see any tension between privacy protections and strong digital trade rules.

Many of the privacy frameworks either that have been proposed here—and we agree, Federal privacy reform is long overdue—or, you know, one of the 19 comprehensive State laws that have been enacted have no tension with either USMCA or the U.S.-Japan agreement. That is because those laws or bills don't enact data localization requirements. They don't restrict the free flow of transfers of information.

And, importantly, within USMCA, there is a pretty clear language that if there should be any tension in the future between domestic regulation and international trade agreements, U.S. law prevails.

Ms. DELBENE. Thank you. And I don't think other nations take the same approach on their own either, which also puts us in a weaker position if we aren't moving forward.

I also, you know, wanted to talk a little bit about intellectual property. Obviously, protecting intellectual property—our intellectual property from adversaries and competitors is essential to keeping our edge and protecting the livelihoods of small business owners across the country, and that is why the U.S. has historically opposed source code disclosure as a condition of doing business in a trading partner country, and we included this production in the broadly bipartisan USMCA.

Dr. Walch, how would you respond to a requirement to disclose your company's source code to a foreign government as a condition of doing business?

Ms. WALCH. Thank you so much for the question.

We would just leave. Part of it is because there is data in our back end that was collected in very carefully controlled IRB-approved studies on human subjects in the U.S. Those people consented, and we protected that very carefully. It is also our edge. It is what gives us a head start globally.

If we had to disclose our models and somebody could just take them and skip all of the work we did and also have access to models trained on U.S. citizen data, that would be just a no-go. It almost certainly would not be worth it for a company of six people, like my company, to operate in a place that requires us to give up our secret sauce.

Ms. DELBENE. And, of course, if your source code was exposed, as you said, others could potentially access that, too, going forward.

Ms. WALCH. That is exactly right.

Ms. DELBENE. So it is—I think this is another conversation we talk about kind of the policies we need to put in place to make sure we are in a strong position. Privacy, obviously, critically important that we move domestically, but also looking at issues to make sure we are protecting IP are going to be important, too.

I just want to thank all of you for being here on this important subject.

And I yield back, Mr. Chairman.

Chairman SMITH. Thank you. I now recognize Mrs. Fischbach for five minutes.

Mrs. FISCHBACH. Thank you very much, Mr. Chair.

And it seems like every time we discuss the Biden-Harris Administration's actions on the world stage, we hear the same thing, the Biden Administration keeps walking away from discussions where America's voice is needed, and we should be an active participant.

I hear it from agricultural producers across my district, I hear it from manufacturers in my district, and today we are here to talk about the administration's failure to protect U.S. interests in our digital economy.

Foreign governments seem to recognize that our current administration will do little to respond to measures that explicitly or implicitly discriminate against American companies. In some cases government agencies, like the Federal Trade Commission, are even sending American officials to help implement policies that directly undermine America's leadership and innovation.

Mr. Atkinson, what sort of impact does that have on other countries considering similar barriers?

Mr. ATKINSON. Thank you, Congresswoman.

Historically, if it wasn't for U.S. leadership, the world economy would be vastly more protectionist, it would be vastly more distorted because it has been U.S. leadership that has been, if not explicitly, then implicitly holding up countries to a higher standard. They know that if they do this, they are sinning. And nobody really wants to sin; at least you don't want to admit you are sinning.

And so the fact that the U.S. has led in all sets—sorts of areas—we led in telecom deregulation globally, we led in IP, we led in digital—that did lead a lot of countries both to resist doing bad things, but also to say, wait a minute, if the U.S. is doing this and they are the leaders, maybe we should be doing that as well.

And what is so troubling, I think, about USTR's decision—and, by the way, I would add that was really a unilateral decision. Both State and commerce, in my understanding, did not support that decision. Both the State Department and the Commerce Department were surprised by that decision and did not agree with that decision. So it is not as if the entire administration has backed away, although that is the—de facto the case.

So by us not pushing forward and insisting that these countries abide by these new rules around digital, we are basically sending a message that gives them *carte blanche* ability to go ahead and do whatever they want because they know that we are not standing up for that anymore. And if we are not standing up for it, why would they bother to take the political risk in their own countries to stand up for that?

Mrs. FISCHBACH. Thank you very much.

Mr. Razis, why is it important that the U.S. not only defend policy provisions that are beneficial to our digital companies, but how can we do a better job in shaping the vision?

Mr. RAZIS. Congresswoman, thank you for the question.

I think we can start by continuing to export gold standard rules like those we find in the USMCA and the U.S.-Japan Digital Trade Agreement. But there is even maybe a more basic step that can start, which is using the National Trade Estimate, for example, in order to catalog data localization requirements and other digital trade barriers that U.S. exporters face.

Now, historically, the NTE has been a really valuable tool for not just U.S. businesses and policymakers for understanding the data localization requirements and other barriers that foreign countries have enacted, but also for sending a signal to our partners that these sorts of practices are unacceptable.

Unfortunately, the most recent NTE, I think we saw about 70 percent drop in the data localization requirements that were referenced and about 80 barriers that were removed from the report altogether. Now, unfortunately, those barriers didn't disappear. They are still there, and they are still challenging U.S. exporters.

So I think even a basic step, such as fulfilling the congressional mandate around the National Trade Estimate, would be a good place to start.

Mrs. FISCHBACH. Thank you very much.

And, Dr. Walch, I am so sorry, I am running out of time. But you talked a little bit about—I believe with Ms. DelBene—about what would happen with the overregulation, and I just was wondering if you had anything to add to that. She was, I think, asking specifically about some things, but I was generally—with this overregulation, what does that do for your company?

Ms. WALCH. Thank you so much for the question.

So we are a team of six. I don't have an in-house lawyer. And every time I talk to my external representation, I am watching the clock.

Overregulation means that we will rely on him even more, and that is a big burden on us. It is not a big burden on the likes of Google or Meta. They are drowning in lawyers.

Mrs. FISCHBACH. Thank you very much. We made it. I had two seconds left. Thank you so much.

I yield back.

Chairman SMITH. Thank you. I now recognize Ms. Sánchez for five minutes.

Ms. SANCHEZ. Thank you to Ranking Member Blumenauer and Mr. Chairman for holding this important hearing.

I represent part of Los Angeles County and, obviously, it is a large creative and technology industry hub of Southern California. And I am very committed to ensuring that our trade policy uplifts U.S. digital businesses and the workers that support them.

Digital has to be part of our engagement with our trading partners, and I also recognize that our trade policies need to be modernized. We can't just rely on the same old trade models that we have been using for decades. I think our digital trade agenda should consider how foreign adversaries, like Russia and China, manipulate and weaponize American data to harm our democracy.

And we also have to consider how AI and automation reshape the workplace as well. There is a lot of moving parts to this.

For instance, while robots have long been used in high-wage markets, we now see them in more lower-wage ones. And a study by the ITIF found that China's manufacturing sector, for example, uses 12 times more robots than that of the United States. And that is not driven by market forces, but it is driven by the Communist Party's generous subsidies.

And that puts our American manufacturing and our American manufacturing workers, which already face an uneven playing

field, at a bigger disadvantage in global trade. So with the rise of new technologies, we need to ensure that our policies prioritize American workers instead of leaving them behind.

Mr. Gottwald, in your written testimony, you touched on the importance of protecting the economic security of the more than five million workers in the creative industries, such as motion pictures, television, and music, which I always say are—our biggest export is our American culture.

Can you expand on how digital trade policy can better ensure that these workers get the compensation and the recognition that they are due?

Mr. GOTTWALD. Thank you, Congresswoman Sánchez.

This is a great question, and it raises very important issues for our union creative professionals, many of whom earn collectively bargained pay and contributions to their health insurance from the sales and licensing of the copyrighted works that they help create. So intellectual property rules are quite important for these workers, their union members, their affiliated AFL-CIO.

So a worker centered digital trade policy, you know, has to extend and address the stolen or unlicensed use of copyrighted content on digital platforms and avoid replicating the outdated and overbroad copyright safe harbor exclusions that exist in some U.S. laws. So one is, you know, let's not do further harm by exporting that model which isn't working here.

And, in addition, they need to address the dangers and downsides to AI that you mentioned, including image-based sexual abuse misappropriation for commercial gain and the proliferation of deepfake videos and other abuses that happen and affect these creative professionals. So thank you for that.

Ms. SANCHEZ. Yes, thank you.

Mr. Atkinson, the U.S. film, television, and streaming industries supports over 816,000 jobs in California and about \$101.7 billion in wages, and I am particularly concerned that some of our closest trade partners are proposing measures that would discriminate against U.S. creative industries.

For example, Australia may require U.S. streaming companies to invest 10 percent of their revenues in Australian content, and Canada wants U.S. streaming companies to subsidize local Canadian news production. These policies could negatively impact my state's and our country's creative industries and the broader U.S. economy.

Could you offer, in the closing seconds that we have, some insight into how these mandates conflict with Australia and Canada's FTA obligations to the United States?

Mr. ATKINSON. Thank you.

I wouldn't use the word would. I would use the—could. I would use the word would. I don't think there is any question that we will have less investment in our creators because of these rules, because of these tax grabs.

Both of our trade agreements should be able to address that. And, again, it requires the USTR, if it is willing to first go over there and negotiate tough within their back pocket to say, we are going to bring a case. Under USMCA arbitration we could bring a

case, under the U.S.-Australia we can bring a case. We just have to let them know that we are not going to do this.

By the way, I would add one other thing where I think I agree with my colleague from the AFL-CIO. We need to make sure that the trade agreements that we have protect creators and allow for site blocking, which is something we have long supported. That we should not allow these foreign websites that are basically pirate sites to be accessible here, and we should have our trade agreements encourage that with other countries as well.

Ms. SANCHEZ. Thank you.

And I yield back.

Chairman SMITH. Thank you. I now recognize the gentleman from Tennessee, Mr. Kustoff.

Mr. KUSTOFF. Thank you, Mr. Chairman. Thank you to the witnesses for appearing today.

Mr. Razis, if I could with you, as it relates to Workday, I understand your company helps to find and hire workers. Can you talk about how Workday helps U.S.-based companies compete globally by providing them with tools to recruit and manage talent across the borders in a competitive digital trade environment?

Mr. RAZIS. Congressman, thank you for the great question.

Workday's business is to help other businesses do well. And so when our customers succeed, we succeed.

In terms of specifics around talent management, a thing that we are very excited about at Workday is a skills-based approach to talent. So we are leveraging AI and other digital technologies to help our customers understand what skills that their existing workforces have, what skill gaps there are in their current workforce that they can grow and help their workers identify, be it in manufacturing, be it in retail or other sectors, and then to identify new sources of talent as well.

And so when our customers are able to leverage Workday products in the AI, especially that is driven there, they are better situated to adapt to new changes in the labor market.

Mr. KUSTOFF. Thank you.

If I can, to follow up maybe, can you talk about how current barriers and regulatory challenges, like the digital service tax, affect Workday's ability to invest in innovation and workforce development here in the United States?

Mr. RAZIS. Of course. So while the digital services taxes are addressed at companies that tend not to be Workday—so we are a business-to-business enterprise, and so—rather than a consumer-facing one.

That said, it speaks to a larger problem and the costs of foreign trade barriers. So in order to overcome a market access barrier like a data localization requirement that requires time and money that could otherwise be invested in additional head count or innovation—and that is—again, that comes with economic costs in addition to the variety of other costs associated with market access barriers.

Mr. KUSTOFF. Thank you. I appreciate the fact that all of you have five minutes to make statements and your written statements are maybe longer than that.

If I could, Dr. Atkinson, with you—because you had a very thorough written statement. Maybe if I can ask you about U.S. Trade Representative Tai's decision to withdraw from, as you say, key digital trade negotiations at the WTO.

Can you explain why she did that, why she withdrew from those negotiations, and does it make any sense to you?

Mr. ATKINSON. So I have not talked to Ambassador Tai, so I will only give you what I can see, sort of, from the outside.

I think there are two factors. And I would add, by the way, I think in the Biden Administration there are forces on sort of the more openness to trade, and there are forces on the less openness to trade. This is not an administration that has one view. I think that is the challenge. As I said, there are folks in commerce who are really pushing for this. There are folks at State who are pushing for this.

I think there are two forces. I think that Ambassador Tai and certain people in the administration, they talk about putting a pause on trade opening and having a middle-class-oriented trade and worker-centered trade. I don't think pause is what—I think pause is a euphemism. I think what they want is a moratorium, if not a rollback.

And they see digital as being this expansive new area and I think, in their view, if they can stop digital trade or slow it down, this could all be—do good.

Now, why do they want to do that? Because there is no question that trade puts limits on our ability. So, for example, we can't tax corporations at 80 percent because they—we could do it for domestic companies. They just raise prices.

But for our foreign—our companies that are trading, if we raise taxes super, super high, they would lose global market share, they would cut workers. So globalization puts—as Tom Friedman once said in his book, they have golden handcuffs. They do limit what we can do domestically, not in any legalistic sense. But if we wanted to, sort of, impose really terrible regulations, they can do that. So I think that is point number one.

I think point number two is there are certain progressives in the Senate in particular who really, really have an animus towards large corporations. They want to sue big corporations, they want to break them up, and they have this narrative that the U.S. economy has become increasingly concentrated, which is a hundred percent false. And I am happy to share that data from the U.S. Census Bureau that shows that simply is not the case.

But in any case, they are having a real animus and a jihad almost against large corporations and big tech in particular.

And I think this was the view, well, if we—somehow, if we go down this path, we are going to limit our ability to break up Google or break up Facebook or sue them. So I think those were the two components of the logic.

Mr. KUSTOFF. Thank you.

I will yield back.

Chairman SMITH. Thank you. I now recognize Mr. Panetta from California.

Mr. PANETTA. Thank you, Mr. Chairman. I had an opening, but I want to follow up on that statement—that eloquent statement. Thank you, Mr. Atkinson for that statement.

But, I mean, does—what about, like, when it comes to global leadership, does the fact that the U.S. participation or lack of, does that also create a vacuum in global leadership, especially when it comes to digital trade rules that could be filled by policies proposed by other trading partners such as Russia or China?

Mr. ATKINSON. Absolutely. Absolutely, Congressman.

The Chinese have a completely—obviously, they have a different vision of governance and government and global governance, and they want to impose their vision and their system on the world. I think Russia is sort of their sidekick, if you will. And this is, basically, a battle for influence.

I have been in countries where the State Department has invited me in, and I see the role of China in these countries. I see China way more active in these countries than we are.

So by us walking away, we are, essentially, giving the Chinese a green light for them to go into these countries and say, hey, look, our system is better. I have talked to Chinese companies who say one of the things that they are really selling, if you will, is we can go in there and give you a turnkey system in an African country that they call safe cities.

Well, what they mean by that is complete total monitoring, complete data collection. They are able to put people into jail for whatever reason you want, and they are selling that system. Where are we? Where are we? Why aren't we in that country saying, by the way, if you do that, it is going to hurt your innovation. And, by the way, it is against human rights. So I 100 percent agree with you.

Mr. PANETTA. Exactly. Mr. Shahbaz, where would you be on that statement?

Mr. SHAHBAZ. I do think it is critical, and I would say that there is two parts to this. So thank you for the question, Congressman.

On the one hand, we do need to make sure that there isn't a vacuum. We do know that the Chinese Communist Party has invested quite a bit, and there was a point where almost a majority of U.N. agencies were led by Chinese nationals. So I think it is very important and it has been great to see the effort that was made, for example, to ensure that it was an American citizen who beat, I believe it was either a Russian or a Chinese national, to lead the ITU, the International Telecommunications Union.

I do think it is great as well that we have stood up now, the Bureau for Cyberspace and Digital Policy, in order to make sure that the United States is active at multilateral fora and through bilateral relations to make sure that we are making the case.

And then I do think—the second point here is what it means domestically. And I think that this has been something that has been pointed out by the other witnesses, is that we need to make sure that our foreign policy is also in line with our domestic policy. And that means that people don't think of the United States as a place that is this kind of anarchy, right?

Because I do think that there is this impression that some of the harms that have come about inevitably from digitalization haven't

been adequately handled by—by domestic regulation or whatever it might be or by companies in some ways.

So I do think it is important that the U.S. leads also through a domestic framework that protects rights of Americans, whether that is on privacy, whether that is on ensuring greater transparency. Because, on the other hand, you do have China that, while all of their legislation on personal data helps for domestic surveillance, they are selling that as a great way of protecting privacy for Chinese citizens.

So I do think it is important that the United States leads with a rights-respecting vision, and that is the counterweight to what China is offering. Thank you.

Mr. PANETTA. Outstanding.

I am going to yield back the remainder of my time, one, because we have votes; I want to give other members time. Two, because those two statements, I think, say it all. Thank you, gentlemen.

Chairman SMITH. Thank you. I now recognize Mr. Steube for five minutes, from Florida.

Mr. STEUBE. Thank you, Mr. Chairman.

From the Industrial Revolution to the digital revolution, America has been the beacon of creativity and technological innovation and advancement. But this leadership is at risk from policies both at home and abroad.

The Biden-Harris Administration's abdication of leadership on this issue has been appalling, and I do not have confidence that Kamala Harris' very detailed policy proposal of joy will be good for American digital competitiveness.

Across the globe, including from our allies, we see bad actors stealing our intellectual property, implementing protectionist policies, stifling data security and privacy and imposing unreasonable barriers that disadvantage American companies. It is essential that we establish and enforce robust digital trade rules to protect American companies, both large and small, from unfair digital practices overseas.

Under the Trump administration, strong progress was made on digital trade in the United States-Mexico-Canada Agreement. USMCA took important steps on e-commerce, algorithms, cyber security, cross-border data flow, prohibiting data localization, and consumer protection. It is important to have strong digital policy. It is equally important that the executive branch enforce these agreements and Congress provide rigorous oversight while responding to the need of policy changes.

I applaud the efforts of Chairman Jim Jordan, whom I sit with on the Select Subcommittee on the Weaponization of the Federal Government to engage with the European Union, which is attempting to impose its own censorship regime on American citizens and companies. The EU is pushing authoritarian policies that will interfere with the American democratic process, and the Biden-Harris Administration is turning a blind eye, perhaps because it will help them politically.

The EU's ever-expanding regulatory censorship effort seeks to impose censorship based on what a European official may deem to be, quote, harmful or disinformation. Failure to comply with the

European authoritarians would impose significant fines on American companies that can amount to billions of dollars.

Mr. Atkinson, can you talk about the censorship and anti-competitive practices that the EU is imposing on American companies?

Mr. ATKINSON. Yes. Thank you, Congressman.

There is no question that the EU has a different standard of speech than the United States does. And we see that now in Britain where there have been people who have been prosecuted in the last two months for simply making posts on social media that are legal but not favored by the government. We would, I hope, never do that in the United States.

We have a tradition of free speech. I forget who said it, but I think it might have been Justice Brandeis, the best disinfectant is more sunlight. The answer to hate speech is free speech.

One of the problems with that regime is that the Europeans don't really have digital platform companies. And so if they are going to go after companies for doing this kind of thing, they are going to go after American companies by default. And what is most troubling about that is the massive fines that they can impose. They could, essentially, bankrupt an American company if they wanted to for just allowing speech that is legal in our country.

And, by the way, I would add this—another component is, one of the key things about speech on the internet is American companies, by and large—maybe with the exception of X, because they have a different view, which is their view; that is fine. But the other American platform companies, they do try to respect domestic rules about speech.

And so it is not like they are saying, oh, we are not going to monitor or filter any speech in Europe. They are doing the best they can. And we can argue whether we like that or not, but they are trying to comply with those rules. And the fact that they can be subject to such onerous fines for making a best effort, I find that quite troubling.

It would be one thing if the companies were just thumbing their nose at the—you know, we are not going to abide by your rules at all, screw you. All right. But they are not doing that. They are doing the best they can, and it is an incredibly difficult process when you are seeing millions and millions of pieces of content on your site every day.

Mr. STEUBE. Mr. Razis, am I pronouncing that correctly? Under the Trump administration, we had a massive overhaul of U.S. trade policy. Can you talk about the effect of the USMCA, that it had on important areas of concern, like data flow, data localization, and algorithms?

Mr. RAZIS. Congressman, thank you for the question.

USMCA, which, you know, we are certainly pleased to see the bipartisan support around USMCA in a lot of these disciplines has—really is the gold standard. It is the 21st Century rule book when it comes to the digital economy right now.

And so to your point, it safeguards the ability of companies to transfer data across borders securely. It allows—it prohibits data localization requirements, and it protects American exporters, like Workday, from arbitrary and discriminatory requirements to trans-

fer source code or algorithms to foreign governments as a condition for market access.

Workday has about 75 percent of its business based here in North America, and so we are certainly beneficiaries of USMCA. However, we are certainly looking to export more into new markets and would benefit from the protections within USMCA and the U.S. Japan agreement.

Mr. STEUBE. Thank the witnesses for being here today. My time has expired.

Chairman SMITH. Thank you. I now recognize Mr. Schneider from Illinois.

Mr. SCHNEIDER. Thank you, Mr. Chairman. And I will be quick because I know we have to get to votes, but I want to thank the witnesses for joining us today and showing your perspectives.

The expansion of digital trade and digital innovation has literally transformed every industry across our economy. As a result, trading digital goods and services has helped create jobs, expand opportunities for small and family businesses, and cultivate innovation in communities across our country.

Just in Illinois, my state, the digital economy supports more than 300,000 jobs and represents nearly \$3.7 billion in digital exports. The digital economy is an important part of our trade infrastructure, and the United States must remain the leader when writing the rules of the road for the future of digital trade.

The expansion of digital trade and the digital economy has accompanied an international discussion around taxing the revenues and profits earned by multinational corporations. While the Organization for Economic Cooperation and Development, OECD, continues its work to reach a consensus on an inclusive digital services tax framework, individual countries have put in place unilateral measures to protect their tax base.

Like many of my colleagues on this committee, as we have discussed today, I am concerned about Canada's decision to move forward with a digital services tax that unfairly punishes American companies. I applaud the Biden Administration for standing up to—up for American businesses and initiating consultations with Canada through the disputes settlement chapter in the U.S.-Mexico-Canada Agreement, and I hope we can continue working together on this important issue.

The U.S. must ensure that competing proposals that impact the digital economy do not undermine American workers, American businesses, or American national security. We cannot seek grant or adversaries on digital trade. Instead, we should lead the way on global technology advancement. I am confident that we can find our seat at the table and work with our allies to establish strong equitable trade digital standards to protect American leadership and innovation.

And with that, I want to ask—well, I have three questions. I am going to focus on one just for time. Mr. Atkinson, in my district I am home to many of the leaders in biopharmaceutical and bioscience sectors, what I call life science corridor through my district. We lead the country; we lead the world. These companies are developing and deploying the next generation of innovative technologies.

Can you discuss how strengthening digital trade laws can improve protections for intellectual property, specifically in the context of medical or life science innovation and discuss the scope of impact if the United States does not provide adequate protections for this important industry?

Mr. ATKINSON. Absolutely. In two ways. One is the biopharmaceutical sector is increasingly data-driven, as you know, using algorithms to develop new kinds of treatments and devices, and a lot of that is going to be cross-border. It is going to be taking patient data from various places, again, totally anonymized. We have to make that point clear. They don't care about the name of the data. They just need to know, does this person have heart disease, what are the indications. So, number one, we need to be able to protect that.

The other is this question of data exclusivity. It is particularly for biologics, large molecule drugs where the patent protection is different. We need to make sure that when we sign trade agreements that we have 12 years of data exclusivity. Because what other countries are doing, they want less data exclusivity, a shorter period of time so they can basically take the molecule that we have developed and then sell it in our market more quickly than they would otherwise when it expires. Both of those issues, to me, are critical.

Mr. SCHNEIDER. Great. And I agree that it is critical. Like I said, we have talked a lot about Canada. We can talk more. We have other issues. This is a critically important issue for our country, for national security.

For the sake of time, Mr. Chair, I am going to yield back my time so we can get Mr. Feenstra in.

Chairman SMITH. Thank you. I now recognize the gentleman from Iowa, Mr. Feenstra.

Mr. FEENSTRA. Thank you, Mr. Chair. Thank you witnesses for being here.

Obviously, we know that we lead the world in innovation when it comes to digital innovation. We also understand that we are seeing other countries impose intellectual property taxes on what we have. Germany has imposed a tax on intellectual property. Canada announced in June that it would retroactively impose discriminatory taxes going back two years. I mean, DST is absolutely at the forefront now of being taxed.

So my question is this. Dr.—Mr. Atkinson, do you see similar types of discriminatory taxes being applied towards Chinese companies or other countries? So—yeah. Are we the only ones here?

Mr. ATKINSON. So I don't think they have designed their systems explicitly to say let's go after the Americans, partly because they—you know, there was that statement that an EU official made. It was one of those things you are only supposed to say in private, but he said it in public.

Mr. FEENSTRA. Exactly, yes.

Mr. ATKINSON. Gave the game away.

Mr. FEENSTRA. Yes.

Mr. ATKINSON. I think he regrets saying that now.

Mr. FEENSTRA. But it came out, and it was real.

Mr. ATKINSON. It came out, and it was very real.

Mr. FEENSTRA. Yes.

Mr. ATKINSON. The issue is why it seems like it is coming at us. Our companies are bigger, and they are more successful. And so they set the thresholds where these regulations, where these taxes and other things kick in. They set the thresholds in a way that pick up a lot of American companies, but the Chinese are just not big enough in those markets yet.

We are very big in Europe, we are very big in Australia, we are very big in Canada. The Chinese aren't yet, the Alibabas, the Baidus, and the like. And so if they were big, they would get wrapped in—wrapped up in this. They are just not big enough, so it is a de facto attack on U.S. companies.

Mr. FEENSTRA. Got you. We can do 301 investigations, we can do countermeasures. I get all that.

But the administration, with Janet Yellen and Treasury, I mean, do you see any sense that they are standing up and fighting against these imposed taxes from Canada and from Germany?

Mr. ATKINSON. I think there is some pushback in the negotiations with regard to Canada. I don't see it with regard to Europe. And I think it is—it is a long-standing problem that U.S.—the U.S. foreign policy establishment in government prior—and the military establishment prioritizes foreign policy and military over U.S. economic competitiveness and technology competitive issues.

Their view, in my opinion, is let's not rock the boat. There is this conflict in Ukraine. We are just going to turn a blind eye to this.

Mr. FEENSTRA. We have become the piggy bank, literally the piggy bank, and really no one is fighting, you know, for just fairness. That is all we want is fairness. And that is not happening.

Thank you. And I yield back.

Chairman SMITH. Thank you. Thank you for yielding back.

Thank you, again, to all of our witnesses. Sorry we have to run out of here because of votes, but I think we will make it.

Please be advised that Members will have two weeks to submit written questions to be answered later in writing. Those questions and your answers will be made part of the formal hearing record.

With that, the subcommittee stands adjourned. Thank you again.

[Whereupon, at 10:52 a.m., the subcommittee was adjourned.]

PUBLIC SUBMISSIONS FOR THE RECORD



September 26, 2024

The Honorable Adrian Smith
Chair
Subcommittee on Trade
Committee on Ways and Means
Washington, District of Columbia 20515

The Honorable Earl Blumenauer
Ranking Member
Subcommittee on Trade
Committee on Ways and Means
Washington, District of Columbia 20515

The Honorable Jason Smith
Chair
Committee on Ways and Means
Washington, District of Columbia 20515

The Honorable Richard Neal
Ranking Member
Committee on Ways and Means
Washington, District of Columbia 20515

RE: Submission for the Record for the Trade Subcommittee Hearing *Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules on Behalf of Morgan Reed, President of ACT | The App Association*

Dear Chairman Smith, Ranking Member Blumenauer, Chairman Smith, and Ranking Member Neal:

Thank you for the opportunity to discuss the importance of protecting American innovation through our trade policies. ACT | The App Association supports your goal of maintaining and expanding United States leadership on digital trade to ensure a strong economy and a favorable market for American small businesses. We believe that the keys to a strong digital trade policy remain opposition to digital trade barriers like the European Digital Markets Act (DMA), Digital Services Act (DSA), and other barriers like digital services taxes, as well as clear rules on cross-border data flows, source code transfer, and data localization.

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.

Further, as explained in a multi-association stakeholder letter led by the App Association to the Biden Administration,¹ our community of small business innovators is deeply concerned with the United States Trade Representative's (USTR's) October 25, 2023,

¹ <https://actonline.org/wp-content/uploads/Small-Business-Ltr-re-USTR-Digital-Trade-3-Nov-2023-w-cosigners-1.pdf>.

announcement of its withdrawal of support for foundational digital trade policies, including those that enable cross-border data flows, avoid forced data localization mandates, protect source code, and ensure that digital products are not unduly discriminated against. The USTR's position significantly impacts U.S. leadership across various global industries and platforms, enabling countries like China to secure their position in and dictate matters on global trade. We are concerned that stepping back on crucial digital trade priorities that support U.S. businesses will set a harmful precedent for other U.S. trade interests. We urge the USTR to reinstate their position for crucial digital trade priorities that allow small and large businesses alike to reliably operate and strengthen the United States as a global powerhouse for important and emerging trade objectives.

The global digital economy holds great promise for small app development companies, but our members face a diverse array of trade barriers when entering new markets. These barriers may take the form of laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. While these barriers have different forms, they all have the same net effect: impeding U.S. exports and investments at the expense of American workers, and particularly of small businesses. In your efforts to support U.S. growth through digital trade policies, we urge for your prioritization of the following:

Cross-Border Data Flows and Data Localization

Many businesses rely on cross-border data flows, and not just those that are considered to be in technology industries. These kinds of entities are often clients and customers of App Association members. For example, a wide range of healthcare entities conduct trials in multiple countries and bring their findings back to their U.S.-based labs. Multinational manufacturers and retailers need to send data from their customers' location to their warehouses during an online order, and small businesses of all kinds rely on cross-border exchange to reach their customers. Forcing businesses to store data inside the borders of a country where they conduct business requires them to either build data centers locally or contract with cloud firms to redirect and send their data on circuitous paths in ways that are needlessly duplicative, expensive, and insecure.

For businesses whose apps are available for download worldwide from the major app stores or the internet, much of their business comes from spontaneous downloads by people who have a need the app fills. If the developer acquires a single user in a country with a data localization requirement, they may need to pay for separate storage and processing of that data in the country, while ensuring that any data pertaining to the single user stays within that country's borders. Requiring this level of data management

adds an unnecessary layer of complexity and is often beyond the technical and financial capacities of businesses.

The United States has historically supported cross-border data flows and opposed data localization mandates in other countries. These positions have allowed American businesses—and especially small businesses—to thrive in global competition through continuous innovation. Upending decades of support for cross-border data flows and opposition to data localization mandates will leave American businesses in the lurch and unable to continue providing strength to our economy. Congress must continue its support of American small businesses by opposing data localization requirements and supporting cross-border data flows.

Digital Trade Tariffs

American App Association members take advantage of the internet's global nature to reach the large portion of their customers who are outside the United States. However, collecting customs duties on digital services directly contributes to the balkanization of the internet and prevents small business digital economy innovators from entering new markets.

Members of the World Trade Organization (WTO) have supported a moratorium on e-commerce tariffs since 1998 and extended the moratorium regularly since then,² including most recently at this year's WTO Ministerial Conference. App Association members and other small businesses need protection from e-commerce tariffs to continue to do business. E-commerce tariffs are trade barriers that give preferential treatment to the narrow set of companies whose digital supply chains stop at national borders. We applaud the U.S. government's contributions to efforts leading to the preservation of the e-commerce moratorium.

Many countries are considering or implementing digital services taxes (DSTs). Canada, for example, recently finalized its version of a DST, which applies to "certain digital services that rely on engagement, data, and content contributions of Canadian users," as well as "certain sales or licensing of Canadian user data,"³ and will charge a three percent tax on those revenues retroactively. For small businesses that rely on licensing of data or user contributions, this could represent a huge portion of their operating expenses. Digital services taxes, like many current barriers to trade, attempt to target large tech companies but will almost certainly sweep in small tech as well. We urge Congress to support the Organisation for Economic Co-operation and Development (OECD)/G20 Inclusive Framework that continues to work addressing taxation.

² Safro, Nana Ama. "A Guide to the WTO E-Commerce Moratorium Debate." Available at <https://www.taxnotes.com/featured-analysis/guide-wto-e-commerce-moratorium-debate/2024/03/01/7j877>

³ "Digital services tax," Canadian government website. Available at <https://www.canada.ca/en/services/taxes/excise-taxes-duties-and-levies/digital-services-tax.html>

Intellectual Property and Source Code Protection

The infringement and theft of intellectual property (IP) jeopardizes the success of App Association members and hurts the billions of consumers who rely on their app-based products and services. Each kind of IP (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which App Association members depend. IP violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone is a potential “end-of-life” occurrence for a small app development company. Strong and fair protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential to their businesses.

Notably, some governments have proposed or implemented policies that make legal market entry contingent upon the transfer of proprietary source code. For app developers and technology companies, the transfer of source code presents an untenable risk of theft and piracy. These requirements present serious disincentives for international trade and are non-starters for the App Association’s members.

Technical Protection Mechanisms, Such as Encryption

Global digital trade depends on technical protection mechanisms, such as strong encryption techniques, to keep users safe from harms like identity theft. However, some governments and companies insist that “backdoors” be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a security and privacy standpoint, the viability of app developers’ products depends on the trust of end users.

Misapplication of Competition and Consumer Protection Laws to Digital Markets

Various regulators, including key trading partners, are currently considering or implementing policies that jeopardize the functionality of nascent and emerging technology markets—most famously, including “digital platforms”—that have enabled countless American small businesses to grow. Since its inception, the app economy has successfully leveraged digital platforms, enabled by lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for developers, among other benefits. Foreign governments regulating digital platforms inconsistent with U.S. law will upend this harmonious relationship enjoyed by small-business app developers and mobile platforms, undermine consumer privacy, and ultimately serve as significant trade barriers.

In the context of digital platforms and other markets, proposed and implemented changes to competition laws present an increasing threat to our members’ growth and

job creation. For example, we remain concerned with a global trend by regulators in both developed and developing trading partners to alter their approach to mergers and acquisitions.⁴ Our members and fellow innovators must be able to look to acquisitions as a key part of building their future through competing in the global digital economy.

Conclusion

Right now, digital trade looks like the Autobahn. Companies can deliver their data and products where they are needed quickly and efficiently. The process is mostly frictionless, and it means companies can compete from a level playing field. Erecting barriers to free digital trade would be like adding toll plazas to the road. It causes jams, slows everyone down, and makes it harder for companies to conduct business. But some companies—large ones with big compliance teams—have an EZ Pass. It's going to be small businesses stuck fishing change out of the cupholder while industry titans, especially those based overseas, sail right through.

I urge you to continue your support for strong digital trade protections for small businesses. The Committee can help small businesses by holding hearings like this one to highlight the importance of strong digital trade protections, working with the United States Trade Representative to continue longstanding support for digital trade, and ensuring small business voices are heard on this issue. I thank the Committee for your strong support of small business.

Sincerely,



Morgan Reed
President

ACT | The App Association

⁴ See our recent open letter regarding recent international trends in competition regulations, available at <https://actonline.org/2024/08/12/an-open-letter-regarding-recent-international-trends-in-competition-regulation/>

Written Testimony Submitted to the Subcommittee on Trade
U.S. House Committee on Ways & Means
118th Congress, Second Session

Amba Kak and Sarah Myers West
Co-Executive Directors
AI Now Institute

*Hearing on "Protecting American Innovation by
Establishing and Enforcing Strong Digital Trade Rules."*

September 2024

AI Now appreciates the opportunity to submit written comments for the record. We are co-executive directors of the AI Now Institute, which is an independent research institution. We do not represent any clients and do not currently take funding from corporate donors, including tech companies whose practices and products our work is dedicated to examining. We strongly support independent, peer-reviewed research and the intellectual freedom and integrity of our community and scholars. Our current funding comes from foundations, listed on our website. In general our funding is structured to support our broad research and policy goals and is not earmarked to specific projects nor does it shape nor dictate our research outcomes.

We view digital trade agreements as the next frontier in tech regulation. Global trade agreements, typically negotiated in secret and without public input or meaningful public or congressional deliberation, could prematurely deter or undercut ongoing efforts to regulate the tech industry. Any digital trade provisions being negotiated proximate to the World Trade Organization (WTO) through the Joint Statement Initiative (JSI) on E-Commerce or in any regional or bilateral context must preserve this policy space and set a more progressive baseline for digital policy.

Trade agreements include binding and enforceable international rules and cooperative frameworks that limit the parameters of how governments can regulate commercial firms. Because of the secrecy of the negotiations and their relative immunity to public political pressure, they have become a focus for intense tech industry lobbying for preferential treatment.

"Digital trade" policy is fast emerging as the next battleground where trade rules could function to prematurely deter or undercut ongoing congressional and regulatory efforts related to establishing policy for data privacy and security, AI policy, and competition in the tech industry.

International trade agreements with broad-reaching rules are a relatively recent creation, having only become widespread in the second half of the 20th Century. Those that extend beyond the traditional trade mechanisms of tariffs and quotas to impose policy mandates and constraints with respect to signatory countries' domestic non-tariff policies are even more recent¹ and arose together with, and very much espoused by, the neoliberal order then emerging.² Per this ideology, policies that directly (or crucially—indirectly) prioritize domestic workers or businesses, or disadvantage foreign ones, even if inadvertently, are deemed to be misguided and risk eventually stifling growth and shrinking the domestic and the global economy.

This consensus is generally operationalized through rules around non-discrimination, such as the “national treatment” principle, which requires that countries do not treat commerce from other signatory countries less favorably than they treat their own.³ For example, the United States may not subject Canadian products to stricter regulation than those that U.S. products are subject to.⁴ Not following these rules has punitive consequences: countries can be sued before trade agreement dispute settlement tribunals, and sanctions can be imposed until non-conforming domestic policies are removed or changed.⁵

While traditional trade barriers focused on quotas and tariffs, more recently trade agreements place strong emphasis on regulation as a potential trade barrier. Over the last few decades, global trade laws have been enforced (via trade agreement dispute-settlement tribunals) to chill and undermine national regulation that pursues other non-trade related policy goals like environmental justice or development.⁶

“Digital trade” or trade agreements that apply to technology-related products and services are emerging as the next battleground where trade rules could function to deter or undercut global regulatory efforts pursuing privacy protection, algorithmic accountability, and competition objectives, among others.⁷ In the United States, this risk is heightened in the current moment: with no federal laws on data privacy, tech sector competition, and algorithmic accountability, but

¹ Burcu Kilic, “Shaping the Future of Multilateralism – Digital Trade Rules: Big Tech’s End Run Around Domestic Regulations,” Heinrich-Böll-Stiftung, last modified May 2021, <https://eu.boell.org/en/2021/05/19/shaping-future-multilateralism-digital-trade-rules-big-techs-end-run-around-domestic>.

² Quinn Slobodian, *Globalists: The End of Empire and the Birth of Neoliberalism* (Harvard University Press, 2018), <https://doi.org/10.1017/eso.2020.12>.

³ “Principles of the Trading System,” World Trade Organization, accessed September 25, 2024, https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.

⁴ Timothy Meyer, “The Political Economy of WTO Exceptions,” *Washington University Law Review* 99, no. 4 (2022): 1299-1370, <https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2280&context=faculty-publications>.

⁵ Burcu Kilic and Renata Avila, “The Multilateral Trade System and the World Trade Organization (WTO): Lesson 101,” Public Citizen, accessed September 25, 2024, <https://www.citizen.org/article/the-wto-101/>.

⁶ Barbara Moens and Karl Mathiesen, “Trade Partners See Red Over Europe’s Green Agenda,” *Politico*, January 16, 2023, <https://www.politico.eu/article/eu-green-agenda-has-its-trading-partners-seeing-red-climate-neutrality/>; David Henderson, “Unlawful Trade Barrier Warning Over Bottle Return Scheme,” *BBC*, February 8, 2023, <https://www.bbc.com/news/uk-scotland-64563015>.

⁷ Kilic, “Shaping the Future of Multilateralism.”

significant bipartisan political momentum across these areas,⁸ any trade agreements signed by the United States that further entrench and expand the privileges the tech industry enjoys could end up prematurely cutting off the U.S. domestic policymaking process and thus the opportunity for Congress, U.S. regulators, and the public to make such interventions.

The tech industry has been quick to recognize and exploit trade policy as a vehicle for regulatory influence. The Trans-Pacific Partnership set the initial blueprint for the Big Tech policy agenda for digital trade, although the United States did not enter into this agreement because it could not obtain majority support in Congress.⁹ The 2015 TPP was the first trade agreement with the sort of digital trade terms sought by industry. It contrasted with various past U.S. free trade agreements that included E-Commerce chapters limited to facilitation of trade in the digital age with rules on digital signatures and online contracts. TPP negotiations went on for six years (2009-2015) behind closed doors and with significant evidence of lobbying by Big Tech, foreclosing the possibility of any robust public input.¹⁰ While the United States remained outside of the TPP, its digital trade chapter (finally published in 2015) provided an initial blueprint for the U.S.-led U.S.-Mexico-Canada (USMCA) agreement that concluded in 2019.¹¹ The USMCA is the only U.S. trade agreement approved by Congress that contains the digital trade rules sought by the tech industry. This agenda reflects the standard policy positions advocated for by Big Tech in national debates, including limiting any restrictions on cross-border data flows and an absolute restriction on data localization (requirements that data be stored within the country), as well as strict protections against government access to source code or algorithms.¹²

The USMCA set a dangerous precedent where the tech industry now looks to trade agreements as an arena where they can lobby to establish policy positions globally, bypassing public scrutiny, before these issues are democratically deliberated in national contexts. In fact, recent analysis by Rethink Trade pointed to a long list of ways in which the USMCA provisions directly contradict emerging policy positioning with bipartisan congressional support subsequently put

⁸ "Text - H.R.3849 - 117th Congress (2021-2022): ACCESS Act of 2021," Congress.gov, June 24, 2021, <https://www.congress.gov/bills/117/congress/house-bill/3849/text>; "Text - S.2992 - 117th Congress (2021-2022): American Innovation and Choice Online Act," Congress.gov, March 2, 2022, <https://www.congress.gov/bills/117/congress/senate-bill/2992/text>; "Text - AB-1651 - California Assembly (2021-2022): Worker Rights: Workplace Technology Accountability Act," California Legislative Information, January 13, 2022, https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651.

⁹ Kilic, "Shaping the Future of Multilateralism"; Peter Baker, "Trump Abandons Trans-Pacific Partnership, Obama's Signature Trade Deal," *New York Times*, January 23, 2017, <https://www.nytimes.com/2017/01/23/us/politics/tpp-trump-trade-nafta.html>.

¹⁰ Mark Wu, "US Should Not Negotiate Free Trade Behind Closed Doors," *Financial Times*, May 26, 2015, <https://www.ft.com/content/28432090-03b3-11e5-a70f-00144feabdc0>.

¹¹ David A. Gantz, "The USMCA: Updating NAFTA by Drawing on the Trans-Pacific Partnership," Baker Institute, last modified February 21, 2020, <https://www.bakerinstitute.org/research/usmca-updating-nafta-drawing-trans-pacific-partnership>.

¹² Thomas Streinz, "Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy," in *Megaregulation Contested: Global Economic Ordering After TPP*, ed. Benedict Kingsbury et al. (Oxford University Press, 2019), 312-342, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784503.

forth by the Biden Administration.¹³ The digital trade terms sought by the tech industry act as a potential deterrent against renewed efforts by the U.S. (or any signatory) government to regulate the tech industry: in order to pass such policies, which might clash with existing trade agreements, they would have to justify why these don't violate current obligations or fall under stated exceptions.

Looking ahead, President Biden and the U.S. Trade Representative (USTR) under the Biden Administration, Katherine Tai, decided that the United States must now take a different approach to trade from the one pursued under the TPP and USMCA.¹⁴ In fact, they have repeatedly advocated for a trade agenda that centers consumer and worker interests,¹⁵ signaling an opportunity to reconceptualize trade agreements as vehicles for setting a higher progressive baseline in favor of greater policy protections and policy space for domestic legislators and regulators, and not just as an anti-regulation tool.

The Biden administration USTR approach to digital trade reflected a recognition that, in the new context of Congress and the White House working on oversight of the digital economy, the U.S. position on digital trade rules needed to respect the role of Congress and U.S. regulators in determining domestic tech policies. In removing the U.S. attributions in support of USMCA-replicating proposals at the WTO JSI negotiations in October 2023 that the previous administration had tabled in 2019, the Biden administration acted to protect domestic federal and state policymakers from having their decisions internationally preempted.

Non-discrimination prohibitions in trade agreements should not be used to protect American Big Tech companies from competition regulation abroad. Such provisions must be crafted to leave policy space for laws aimed at enhancing competition, even where they might disproportionately impact American Big Tech firms.

The TPP and USMCA "non-discrimination" requirements were so broadly worded that the provision could be interpreted as restricting member countries from enacting policy that, while neutral on its face, effectively has a greater impact on firms from a particular country. In the context of antitrust or other pro-competition regulation, this could mean therefore that competition regulation which disproportionately impacts American Big Tech (because of their

¹³ "Big Tech 'Digital Trade' Plan for IPEF Could Undermine Key Congressional and Administration Privacy, Anti-Monopoly, and AI Accountability Initiatives," Rethink Trade, last modified January 23, 2023, https://rethinktrade.org/wp-content/uploads/2023/01/2023.01.23-Conflicts-between-key-digital-proposals-and-prospective-IPEF-digital-trade-terms_for-lay-out-003.pdf.

¹⁴ Claude Barfield, "US Indo-Pacific Policy Prioritises Security Over Economics," *East Asia Forum*, February 10, 2023, <https://www.eastasiaforum.org/2023/02/10/us-indo-pacific-policy-prioritises-security-over-economics/>; "US Trade Representative Tai Hints at New Asian Economic Framework - NHK," *Reuters*, November 18, 2021, <https://www.reuters.com/world/asia-pacific/us-trade-representative-tai-hints-new-asian-economic-framework-nhk-2021-11-18/>.

¹⁵ Jeanna Smialek, "Ambassador Tai Outlined Biden's Goal of Worker-Focused Trade Policy," *New York Times*, June 10, 2021, <https://www.nytimes.com/2021/06/10/business/economy/us-trade-katherine-tai.html>.

dominance, size, scale, and data advantages) could be seen as violating the non-discrimination diktat of the trade agreement.

This risk is not hypothetical. We've already seen Apple and Google wield this argument in the context of South Korea's 2021 law targeting anti-competitive app store policies, on the grounds that it has a discriminatory effect because of its disparate impact on U.S. firms.¹⁶ Rethink Trade also published a report that reviews corporate submissions to the annual USTR Trade Estimates Report of trade barriers that reveals a pattern of corporate lobbying using broad "non-discrimination" arguments to urge USTR to undermine other countries' competition regulation.¹⁷ Other non-Big Tech companies in the industry are also chiming in: in a recent letter to the USTR titled "Don't let Big Tech Manipulate Trade Policy to Kill Competition," the Coalition on App Fairness—whose larger members include Spotify and Epic Games—urged the USTR not to follow the USMCA/TPP approach and ensure that digital trade rules do not provide a basis for U.S. big tech monopolies to attack legitimate anti-monopoly policies in other countries as "illegal trade barriers"¹⁸ These efforts all point to the wave of competition-focused regulation being proposed in the United States, along with the Biden Administration's declaration not to "tolerate domestic monopolies" as further reason not to entrench contradictory positions in global trade fora.

Much of the impact of the non-discrimination provision will be determined by its precise wording. In the South Korea app store case, Apple and Google's complaint to the U.S. government wasn't a credible legal threat given that KORUS (the Korea-U.S. trade agreement) did not have the TPP/USMCA-style of non-discrimination clause and so the trade pact-based challenge to the law remained conceptual. This only underscores the importance of ensuring carefully tailored language that avoids the pitfalls of the TPP in future agreements.¹⁹ Rethink Trade draws on the language in KORUS to propose a variation that preserves space for such pro-competition policy, by clarifying that a country will not be in violation "merely because" it results in differential effects on a particular country's products and instead must have the "objective or predominant intent to afford protection."²⁰

Expansive and absolute secrecy guarantees for source code and algorithms in trade agreements could undermine the direction of algorithmic accountability policy in the

¹⁶ David McCabe and Jin Yu Young, "Apple and Google's Fight in Seoul Tests Biden in Washington," *New York Times*, August 23, 2021, <https://www.nytimes.com/2021/08/23/technology/apple-google-south-korea-app-store.html>.

¹⁷ Daniel Rangel et al., "Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies," Rethink Trade, last modified November 1, 2022, <https://rethinktrade.org/wp-content/uploads/2022/11/20221101-AELP-DocLayout-v7.pdf>.

¹⁸ Coalition for App Fairness to Ambassador Tai: Don't let Big Tech Manipulate Trade Policy to Kill Competition," Coalition for App Fairness, last modified January 11, 2023, https://appfairness.org/wp-content/uploads/2023/01/20230111_USTR-IPEF-CAF-Letter.pdf.

¹⁹ Rethink Trade's submission on IPEF [Currently on file with author will be public later]

²⁰ Rethink Trade's submission on IPEF [Currently on file with author will be public later]

United States and globally, which is moving towards more proactive and continuous monitoring of artificial intelligence (AI) systems.

Expansive and absolute secrecy guarantees for source code and algorithms are another key feature of the industry-backed USMCA approach. These provisions are justified as preventing the forced transfer of software trade secrets as a condition for market access (a concern animated primarily by Chinese actions in the past),²¹ but the broadly worded protections effectively risk preventing government oversight over algorithms wholesale, and especially so when they involve proactive monitoring and are not in response to a specific court order.

This contradicts the direction of algorithmic accountability policy globally (including multiple proposals in the United States) that is moving towards more proactive and continuous monitoring of AI systems, especially in sensitive or high-risk domains.²² Several organizations have pointed out that the USMCA definition of “algorithm” is broad enough to restrict the sharing of even mere descriptions of algorithms with regulators, a key part of algorithmic transparency proposals such as AI registries.²³ This could have impacts across a range of proposals such as regulatory evaluation of AI including those addressing worker surveillance, anti-competitive self-preferencing, and bias and discrimination. In their digital trade policy paper, the AFL-CIO, argued that any USMCA-style source code/algorithm secrecy provision would operate to “prevent the protection of workers from the excesses of algorithmic management.”²⁴

Achieving such expansive secrecy guarantees remains a consistent lobbying priority for the tech industry. A broadly worded protection for source code and algorithms risks seriously undermining efforts for algorithmic accountability both in the United States and abroad and must be prevented.

Beyond these defensive approaches, there is also potential for the IPEF and forthcoming trade policy to set a more progressive baseline on these issues.

²¹ Keith Bradsher, “How China Obtains American Trade Secrets,” *New York Times*, January 15, 2020, <https://www.nytimes.com/2020/01/15/business/china-technology-transfer.html>.

²² “Text - S.797 - 117th Congress (2021-2022): PACT Act,” Congress.gov, March 17, 2021, <https://www.congress.gov/bill/117th-congress/senate-bill/797/text>; “AB-1651 (2021-2022): Worker Rights: Workplace Technology Accountability Act,” California Legislative Information; “Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work,” EUR-Lex, December 9, 2021, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52021PC0762>; “Text - H.R.6580 - 117th Congress (2021-2022): Algorithmic Accountability Act of 2022,” Congress.gov, February 4, 2022, <https://www.congress.gov/bill/117th-congress/house-bill/6580/text>; “The Digital Services Act Package,” European Commission, accessed September 25, 2024, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>; “AB-1651 (2021-2022): Worker Rights: Workplace Technology Accountability Act,” California Legislative Information.

²³ “Public Citizen Comments: Trade Policy in the Digital Economy Hearing,” Public Citizen, last modified December 14, 2022, <https://www.citizen.org/article/public-citizen-comments-trade-policy-in-the-digital-economy-hearing/>.

²⁴ Patrick Woodall, “Testimony Before the Subcommittee on International Trade, Customs, and Global Competitiveness, Hearing on ‘Opportunities and Challenges for Trade Policy in the Digital Economy,’” Senate Finance Committee, last modified November 30, 2022.

The aspiration towards a more proactive stance is somewhat constrained by the fact that, despite growing momentum, the United States lacks enforceable federal policy on issues like privacy, surveillance, competition, and algorithmic accountability. In the absence of a clear regulatory benchmark, how is USTR to advocate in favor of any baseline standard? That said, even non-binding language that highlights the need for global consensus in favor of clear limits on commercial and worker surveillance; algorithmic accountability; and in favor of competition regulation would represent a major departure from the USMCA model, one that opens up the possibility of trade law as a vehicle for pushing forward (rather than against) tech accountability.



1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

CTA Statement for the Record

House Ways and Means Committee Trade Subcommittee

September 20 Hearing on Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules

October 4, 2024

The Consumer Technology Association appreciates the opportunity to submit a statement for the record for this important hearing. Digital trade enables the success and competitiveness of consumer technology firms of all sizes. Strong digital trade rules - and enforcement of those rules by the U.S. government - disproportionately benefits small business and startups. As several witnesses testified during the hearing, complying with multiple data localization requirements and software source code disclosure mandates is burdensome, overly complex, prohibitively expensive, and potentially dangerous to the health of companies.

Addressing barriers to digital trade should be a high priority for the U.S. government. Sadly, the Office of the U.S. Trade Representative instead has deprioritized addressing barriers to digital trade, taken a still ongoing pause on negotiations on digital trade, and encouraged other governments to discriminate against U.S. technology firms. By contrast, the U.S. International Trade Administration¹ and the Department of State² both continue to prioritize digital trade in their work and will defend the digital trade interests of U.S. companies in other markets. If USTR won't include barriers to digital trade in the statutorily mandated National Trade Estimate report³ on significant barriers to U.S. trade in 2025, we urge ITA and State to include any barriers identified by U.S. industry in their own reports and endeavors. The multi-association memo to the Congress from April 2024⁴ is indicative of the types of barriers to trade that USTR is ignoring but which other U.S. government agencies should address.

Furthermore, data and [More companies are deploying](#) digital tools are increasingly critical to manufacturing processes across all industries, enabling production and supply chain operations across agriculture, healthcare, and other vital sectors of the American economy. However, if USTR does not negotiate and enforce strong protections for software source code and algorithms forming the backbone of technological advancement, the competitiveness of these sectors will

¹ <https://www.trade.gov/press-release/international-trade-administration-announces-efforts-advance-us-competitiveness-and>

² <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>

³ <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/march/ustr-releases-2024-national-trade-estimate-report-foreign-trade-barriers>

⁴ <https://www.technet.org/media/technet-led-multi-association-memorandum-to-congress-expresses-concerns-with-the-ustrs-2024-national-trade-estimate-report/>

Consumer Technology Association*
Producer of CES*

inevitably suffer. Such an outcome would undermine U.S. companies of all sizes and harm broader American economic success. These digital tools that drive innovation include U.S. technology and software, which U.S. companies are often exporting to other markets. This underscores why strong digital trade rules are essential to ensuring that the United States remains the global technology and innovation leader.

For these reasons, CTA urges the subcommittee to organize another hearing with U.S. government leaders from ITA and State who are willing to do the job that USTR cannot. We encourage the subcommittee to ask these leaders what they need, how the Congress can support them, and how they can reflect the views of industry stakeholders - especially startups and small businesses - in their work. Lastly, we urge the Committee to file its own comments with USTR on the NTE by the October 17 deadline⁵, demanding that USTR include barriers to digital trade in the 2025 NTE and that USTR cease its pause and get back at the negotiating table to advance high standard digital trade rules, such as those in the USMCA, in all its bilateral, regional, and multilateral negotiations.

⁵ <https://www.federalregister.gov/documents/2024/09/03/2024-19694/request-for-comments-on-significant-foreign-trade-barriers-for-the-2025-national-trade-estimate>



October 4, 2024

The Honorable Jason Smith
Chairman
U.S. House Committee on Ways and Means
Washington, DC 20515

The Honorable Adrian Smith
Trade Subcommittee Chairman
U.S. House Committee on Ways and Means
Washington, DC 20515

RE: Statement for the Record: Subcommittee on Trade Hearing on Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules

Dear Chairmen Jason Smith and Adrian Smith:

Public Citizen¹ welcomes the opportunity to provide a written statement for the record for the Subcommittee on Trade Hearing on Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules.

As technology has grown to play an ever more important part in our societies and economies, a small number of companies (Big Tech) have emerged as the dominant architects of the global digital system, shaping how content is circulated, services are performed, and infrastructures are designed. Having enjoyed the benefits of a lack of oversight and regulation over the past two decades, these companies have created business models based on a system of mass corporate surveillance that invades people's privacy and have used their economic might to diminish competitors, discriminate (typically unintentionally) against vulnerable populations, and concentrate enormous political and economic power. The rise of Big Tech has inarguably contributed to a surge in wealth and income inequality within and between countries.

The Biden administration and Congress have been grappling with how best to regulate Big Tech to protect consumer privacy, to ensure adequate competition, and to hold companies accountable for discriminatory practice. This has translated into the trade realm as a necessary reversal of previous government policy that sought to push digital trade terms that were

¹ Public Citizen is a nonprofit consumer advocacy organization with more than 500,000 members and supporters. A mission of the Global Trade Watch division is to ensure that, in this era of globalization, a majority of people can enjoy economic security; a clean environment; safe food, medicines and products; access to quality affordable services; and the exercise of democratic decision-making about the matters that affect their lives. We have conducted extensive analysis of U.S. trade and investment agreements and their outcomes, starting in 1991 during the initial North American Free Trade Agreement (NAFTA) negotiations. More recently, Public Citizen has been a leader in working to hold Big Tech accountable in the United States by identifying the dangers of so-called "digital trade" rules with respect to efforts to regulate the tech industry around the globe.

favorable to Big Tech companies by limiting the ability of governments to regulate their business practices.² These corporate-friendly rules sought to:

- Limit the ability of governments to regulate where Big Tech firms send and store consumer data;
- Undermine investigation of discriminatory source code and algorithms, intrusive surveillance practices, and violent incitement online via prohibitions on technology transfer requirements and “trade secrets” protections;
- Shield online platforms from corporate accountability via overly broad liability waivers similar to the controversial Section 230 of the 1996 Communications Decency Act;³
- Manipulate “trade” tools of “market access,” “trade discrimination,” and “conditions for business” to exploit workers in the gig economy; and
- Protect monopolies and promote further consolidation by banning certain pro-competition policies.

These “digital trade” terms are not focused on remedying actual problems related to the online sale of imported goods, such as tariff evasion and product safety, but instead seek to undermine the stronger Big Tech accountability rules of many of our trading partners. In practice, they tie U.S. policymakers’ hands for future regulatory efforts.

In May 2023, Public Citizen joined prominent civil rights organizations such as the Leadership Conference on Civil and Human Rights (LCCHR), the American Civil Liberties Union (ACLU), the Lawyers Committee for Civil Rights Under Law (LCCRUL), and the NAACP to raise concerns about trade provisions that guarantee digital firms new secrecy rights over source code and algorithms. These rules could thwart potential algorithmic impact assessment and audit requirements, such as testing for racial bias or other violations of U.S. law and regulation.⁴

Later that year, we — along with domestic and international consumer protection and digital rights groups as well as a number of small and medium enterprises — were pleased that the Biden administration took these and other consumer concerns into account when the U.S. Trade Representative (USTR) announced it was withdrawing support for controversial digital trade provisions at the World Trade Organisation (WTO) Joint Statement Initiative on E-Commerce (JSI).⁵ We also support the forward-thinking vision of digital trade articulated by the

² Sarah Grace Spurgin, “Public Submissions to U.S. Government Reveal Corporate Wishlist for IPEF: More Power at Our Expense,” Public Citizen, published May 20, 2022, <https://www.citizen.org/news/public-submissions-to-u-s-government-reveal-corporate-wishlist-for-ipef-more-power-at-our-expense/>

³ Anna Edgerton, “Tech Liability Shield Has No Place in Trade Deals, Groups Say,” Bloomberg Law, May 27, 2021, <https://www.bloomberg.com/news/articles/2021-05-27/tech-liability-shield-has-no-place-in-trade-deals-groups-say>

⁴ American Civil Liberties Union, Public Citizen, Centre for Democracy and Technology, et al., “Letter to President Biden”, May 23, 2023, https://www.washingtonpost.com/documents/eea26d7a-08ef-4687-a4ba-c26e38ad7ffe.pdf?itid=ik_inline_manual_44

⁵ Digital Trade Alliance, “Consumer & Digital Rights Groups Call On Governments to Better Protect People’s Fundamental Rights in Trade Deals,” January 30, 2024, <https://dtalliance.org/wp->

USTR, as well as the broad discussions being carried out with multiple stakeholders (including civil rights groups, trade unions, etc.) with respect to framing a new digital trade policy that is grounded in how trade policy affects regular people: consumers, workers, and smaller innovators. We reiterate our willingness to work with the administration to create new digital trade rules that promote worker rights, consumer privacy, civil rights, and data security goals.

Limiting Regulatory Autonomy:

We note that the USTR in its announcement of October 3, 2023, correctly pointed to the need to preserve congressional autonomy to ensure that the digital ecosystem can be regulated in the interests of all stakeholders.

Contrary to what is claimed by many industry lobbyists, extreme digital trade provisions of the kind seen in the U.S.-Mexico-Canada Agreement (USMCA) would significantly limit the ability of domestic lawmakers and regulators to implement consumer protection or other public interest regulation to the digital ecosystem. As aptly described by Mr. Eric Gottwald, Policy Specialist on Trade and Economic Globalization for the AFL-CIO, in his testimony before this Committee, we are not faced with a binary choice between digital authoritarianism and a totally unregulated data marketplace. There is a need for well-tailored regulation, which allows Congress to hold Big Tech companies responsible for unethical data processing and other harmful practices. However, extreme digital trade provisions as seen in the USMCA impose a regulatory straitjacket, restricting the ability of Congress to act in citizens' interests.

For example, the data flow and localization provisions in the USMCA would limit the ability of lawmakers to appropriately secure their citizens' data against unauthorized or unlawful exposure or processing, or against cybercrime, accidental loss, destruction, or damage. Under these provisions, consumers would have no guarantee that their data would be sufficiently protected upon export, even if domestic laws require such protections. Further, countries that have superior privacy laws could see their data protection rules undermined. This would significantly limit any U.S. congressional efforts to enact strong privacy rules for Americans.

Steps taken by the administration, such as the recent executive order⁶ to limit the export of U.S. data to countries of concern, could be challenged under the most extreme data flow rules. Further, as demonstrated by the European Union's objections to extreme data flow provisions at

[content/uploads/2024/01/JSI-Civil-Society-Letter-2024.pdf](#); Citizens Trade Campaign, Accountable Tech, AI Now Institute et al., "Letter thanking president Biden for withdrawing US support for Extreme 'Digital Trade' Provisions," February 2, 2024, https://www.citizenstrade.org/ctc/wp-content/uploads/2024/02/DigitalTradeThankYouLetter_020224.pdf; Coalition for App Fairness, "Letter to President Biden," November 15, 2023, <https://appfairness.org/coalition-for-app-fairness-applauds-biden-harris-administrations-withdrawal-from-digital-trade-negotiations/>

⁶ The White House, "President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," February 28, 2024, <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/>

international trade fora including the WTO JSI, strong privacy rules cannot coexist with free flow of data provisions as exemplified by the USMCA.

Similarly, USMCA-style provisions that limit the ability of public authorities and independent researchers to access source code of algorithms to instances of known violations of law would affect how congressional committees, scholars, and public investigators could review code and related data to identify discrimination and other malpractices that may be baked into AI systems that are increasingly ubiquitous in both the private and public sectors.

Rather than shield these “trade secrets” from public scrutiny, continuous, independent oversight and transparency is key to ensuring human and civil rights are maintained in the digital age. This has been recognized repeatedly in global fora and by the U.S. government, and it has been demonstrated by recent agreements signed between the U.S. government and the AI companies Anthropic and Open AI. These agreements would allow the U.S. AI Safety Institute access to AI models for safety testing both before and after their public release.⁷ While in these cases the companies concerned voluntarily agreed to safety audits, it is not a stretch to imagine the need to implement regulation to require disclosure of AI algorithms (and their source code) in other contexts. Any digital trade provisions that limit such an ability will be detrimental to user safety and the continued development of the AI ecosystem.

Extreme digital trade rules as exemplified by the USMCA would also limit the ability of lawmakers and regulators to implement pro-competition regulation in the digital ecosystem. As seen in the 2020 Report of the House Judiciary Committee’s Subcommittee on Antitrust, Commercial, and Administrative Law as well as several subsequent bills brought to Congress, there is bipartisan support in the U.S. Congress to combat various anti-competitive business practices of Big Tech companies.

This is not only a domestic issue, as a number of jurisdictions are attempting to implement regulations aimed at creating fairer digital marketplaces globally. Big Tech companies have however sought to stifle any attempts at pro-competition regulation through the (mis)use of “non-discrimination” related digital trade provisions.

U.S. Big Tech companies have argued that other countries’ enforcement of their domestic laws are “discriminatory” if such laws affect U.S. Big Tech companies more than the tech companies from other countries, even if those laws are designed to affect any company with extensive market power. This has been seen, for instance, in the pushback against the EU’s Digital Markets Act, South Korea’s App store-related regulation and, more recently, in criticism of South Korean proposals to implement a Platform Fair Competition Promotion Act. Similar pro-digital competition laws are being debated in several countries across the world, from Brazil to India. More often than not, attempts at addressing market concentration affect U.S. firms

⁷ Lauren Feiner, “OpenAI and Anthropic will share their models with the US government,” August 29, 2024, <https://www.theverge.com/2024/8/29/24231395/openai-anthropic-share-models-us-ai-safety-institute>

disproportionately due to the fact that these firms do indeed monopolize various digital markets, frequently to the detriment of consumers. The U.S. should lead regulatory developments aimed at ensuring a level playing field in the digital economy rather than undermining efforts by other nations.

The U.S. government has a long history of intervening to regulate concentration in markets where this could threaten consumer interests or general economic welfare. Therefore, “digital trade” rules must not include terms that forbid countries from establishing or maintaining policies that limit the size or range of services offered by companies, limit the legal structures under which they may be required to operate, or restrict the regulation or break-up of Big Tech monopolies whether American or foreign. Rather than seeking to misuse trade concepts to enable the continued monopolization of digital marketplaces, Congress should have the ability to learn from the regulatory frameworks being implemented in other jurisdictions so as to take action on the domestic front. We reiterate that targeting policies aimed at ensuring a level playing field in the digital ecosystem does not serve the interests of small and medium American enterprises. A coalition of small businesses have in fact pointed out that “the preservation of fair and competitive markets should play a central role in the United States’ foreign trade goals, law, and policy” and accordingly note that U.S. trade policy must be in harmony with the U.S. government’s domestic work to address the anticompetitive conduct of digital gatekeepers.⁸

While some have argued that public interest regulation can be implemented using the public policy exceptions provided in trade agreements, the use of such exceptions in practice is notoriously difficult. A Public Citizen study found that only two such attempts out of 48 have ever proven successful in defending domestic policies at the WTO.⁹ Relying on poorly drafted and legally uncertain exception clauses in trade agreements limits U.S. sovereignty and the ability of our lawmakers to make decisions in the interests of all domestic stakeholders.

As highlighted by Mr. Gottwald, in his testimony before this Committee, digital trade rules have profound implications for the lives of workers in the United States. The changing social and economic dynamics occasioned by the use of emerging technologies implies that it is vital for Congress and regulators to retain the ability to implement public interest regulation. For example, the use of technology has significantly changed the worker-management relationship. Workers are subject to fine-grained surveillance, algorithmic management, and the precariousness occasioned by gig work. There is therefore a need for new regulatory interventions that can re-balance this increasingly skewed relationship between workers and employers. Preserving regulatory autonomy can enable Congress to pass laws to protect workers’ privacy, ensure that algorithmic management systems are designed in accordance with

⁸ Coalition for App Fairness, “Letter to President Biden,” November 15, 2023, <https://appfairness.org/coalition-for-app-fairness-applauds-biden-harris-administrations-withdrawal-from-digital-trade-negotiations/>

⁹ Daniel Rangel, “WTO General Exceptions: Trade Law’s Faulty Ivory Tower,” Public Citizen, February 4, 2022, <https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/>

high labor standards, and prevent non-discrimination-related rules from being used to challenge safety and other pro-labor regulation.¹⁰

Taking the Leadership in Crafting an Inclusive Digital Trade Vision

Rather than abandoning leadership at international trade negotiations, the change in U.S. position has demonstrated that the administration is willing to balance the needs and interests of a diverse group of stakeholders rather than merely adopting the wish list of Big Tech companies. Indeed, the administration has not pulled back from negotiations at various trade fora but has sought to articulate a new vision by enabling the regulation of the digital ecosystem in the public interest, rather than baking in a deregulated ecosystem that could continue to expose Americans to a range of harms. This is also seen in how the 2024 National Trade Estimate (NTE) Report recognizes that countries have a right to implement public interest regulation over the technology ecosystem.

We therefore commend the USTR for taking the leadership to update digital trade rules to provide the policy space necessary for our nation to enact urgently needed policies that Congress and regulators are currently crafting regarding online competition, gig worker rights, online consumer privacy and data security protections, and AI accountability measures.

We also recognize the need for the USTR to build on the improvements made in the 2024 NTE Report (compared to past versions). It is a welcome change that the report is no longer simply a hit list of other countries' laws and regulations that large U.S. corporations dislike. Now, for the first time in memory, USTR is recognizing that it is not in the U.S. national interest to attack and threaten other nations' consumer and worker protection measures. As governments around the world, including our own, work to regulate the rapidly changing tech space, it does not make sense to list new public interest regulations as "barriers to trade."

The Need for Pro-Consumer Rules

There are some legitimate international trade concerns associated with e-commerce and the broader digital economy that should form the bedrock for U.S. policy in any trade negotiations. If digital trade rules are to be included in a trade agreement, they should ensure that goods and services purchased online across borders meet labor, environmental, and consumer safety standards, including by raising de minimis levels so that, for instance, the four million packages arriving from China to the U.S. daily to fulfill online orders can no longer evade U.S. inspection regimes.¹¹ They should prevent corporate misclassification so that so-called "digital platforms"

¹⁰ AFL-CIO, "A Worker-Centred Digital Trade Agenda," February 7, 2023, <https://afcio.org/worker-centered-digital-agenda>; Digital Trade Alliance, "A Primer on the Intersection of Labor Rights, Technology and Trade," October 1, 2024, <https://dtalliance.org/2024/10/01/a-primer-on-the-intersection-of-labor-rights-technology-and-trade/>

¹¹ Rep. Earl Blumenaur, Rep. Rosa DeLauro, Rep. Suozzi, "DeLauro, Blumenauer, Suozzi Release Letter Signed by Majority of House Democrats Urging President Biden to Use Executive Authority to End

involved in transportation, hospitality, healthcare, retail, education, and other industries cannot evade labor, consumer, and other regulations imposed on “brick-and-mortar” businesses. We reiterate the comments of Mr. Gottwald to the Committee that the USTR needs to develop clear labor standards and benchmarks for trade deals. Moving forward, all trade agreements must be designed to ensure high labor standards, which would benefit not just workers in the U.S. but also abroad.

To combat the growing high-tech discrimination in artificial intelligence, international trade rules should guarantee access to source codes and algorithms by congressional committees, government agencies, academic scholars, labor unions, and nongovernmental organizations. Any rules should also introduce corporate liability for personal data collected via computers, cell phones, and the “Internet of Things” without consumers’ explicit, informed permission, shared or sold without their permission, and/or stolen.

U.S. leadership could also move the needle on various broader issues that could enhance trust in the digital economy. Building consensus on issues such as access to the internet or preventing internet shutdowns, enabling global cooperation towards fair taxation of the digital economy (thereby avoiding the multiplicity of digital services taxes), amongst other issues could benefit both U.S. companies as well as citizens from around the world.

Transparency and Oversight

While the USTR’s move away from a number of problematic “digital trade” provisions is a welcome change, it will continue to be necessary for Congress and the public to monitor and publicly debate any future textual proposals on digital trade terms in the context of the WTO JSI on E-Commerce, the Indo-Pacific Economic Framework, U.S.-Kenya STIP or other trade negotiations to ensure they do not become tools for weakening, preventing, or dismantling labor, consumer, or other public interest policies in the digital sphere.

In order for Congress to exercise its constitutional authority over the regulation of foreign commerce, Fast Track Trade Promotion Authority (TPA) must not be renewed. TPA is an extreme delegation of Congress’ constitutional trade authority. It empowers a president to choose prospective trade partners, negotiate deals, and sign trade pacts all before Congress has a vote on any element of it. TPA also empowers the executive branch to control Congress’ voting schedule, and both the House and Senate are required to vote on a trade agreement’s implementing legislation within 90 days of the White House submitting it. No floor amendments are allowed, and debate is limited, effectively eliminating the transparency, accountability, and oversight necessary for the far-reaching trade and investment agreements that the administration is negotiating.

Dangerous De Minimis Trade Loophole,” Press Release, September 11, 2024,
<https://tinyurl.com/v37sr6am>

Instead, Congress should insist that the USTR and the Department of Commerce replace the past secretive trade negotiation process with an on-the-record public process, including public hearings (advertised sufficiently in advance), to formulate U.S. positions and to obtain comment on draft and final U.S. text proposals. After each negotiating session, U.S.-proposed texts and draft consolidated texts must be made public. Strict conflict of interest rules must be enforced. Only by issuing detailed goals and making draft texts available will the American public know in whose interest the negotiations are being conducted.

Conclusion

As governments worldwide work to address fundamental issues relating to digital governance and build a framework for the future, these important policy debates and decisions that will shape every facet of our lives must not be constrained, undermined, or preempted via trade pacts or policies.

To achieve a worker-centered approach to trade that will complement the administration's efforts to build a more resilient economy, its "digital trade" agenda must not undermine domestic policy space on critical emerging issues like AI regulation, gig economy worker protections, discrimination and algorithm transparency, corporate liability, and consumer privacy, but instead should be structured to raise the floor to help ensure that human and civil rights are protected at home and around the globe.

The USTR under the Biden administration has taken important steps in the right direction to rebalance the interests of Big Tech companies with important public interest goals, but there is still work to be done to ensure that Big Tech companies do not inappropriately use trade rules to target other countries' legitimate public policy regulations.

**Written Testimony Submitted to the Subcommittee on Trade
U.S. House Committee on Ways & Means
118th Congress, Second Session**

**Lori Wallach
American Economic Liberties Project's Rethink Trade Program**

*Hearing on "Protecting American Innovation by
Establishing and Enforcing Strong Digital Trade Rules."*

October 3, 2024

Thank you for the opportunity to submit written comments for the record. I am the director of Rethink Trade, a program of the American Economic Liberties Project. Economic Liberties is a think tank and advocacy organization focused on addressing concentrated economic power in the United States. Rethink Trade promotes trade policies that can deliver benefits to most Americans via resilient supply chains and fair markets, the creation and support of good jobs with workers empowered to earn decent wages, public health and safety, and the ability for those who will live with the results to shape the policies affecting their lives.

I am submitting comments to provide a different perspective on representations made at the hearing related to the text or meaning of relevant trade pact terms and recent developments, including the Biden administration's October 2023 withdrawal of U.S. attributions from a draft text of a digital trade pact called the Joint Statement Initiative on E-Commerce (JSI) being negotiated proximate to World Trade Organization (WTO).

1. [The Biden Administration's Digital Trade Moves at the WTO JSI Safeguarded Congress from Prospective International Preemption, Including of the *Protecting Americans' Data from Foreign Adversaries Act of 2024* that Passed the House 414-0 in March 2024.](#)

On March 20, 2024, the House passed the *Protecting Americans' Data from Foreign Adversaries Act of 2024* by 414-0.¹ It was signed into law in April 2024 as part of a broader national security package. The law forbids data brokers from sending U.S. residents' personal data to countries of concern, such as China and Russia. Notably, both China and Russia are part of WTO JSI talks. Thus, it was startling to hear committee members attack Biden trade officials for withdrawing U.S. support for proposed JSI terms that would have designated the U.S. data brokers law as an illegal trade barrier and empowered those two countries to use a trade pact to attack the policy. The proposed text in question forbids governments from restricting the cross-border movement of data, which is precisely what the U.S. law does. The proposal replicated language in the U.S.-Mexico-Canada Agreement (USMCA), which requires: "*No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.*"² A witness at the hearing claimed that a "public policy exception" in the proposed text would preserve regulatory space. In fact, the relevant exception cynically replicated General Agreement on Tariffs and Trade (GATT) Article XX language that has been rejected by WTO tribunals in 46 of 48

¹ "Actions - H.R.7520 - 118th Congress: Protecting Americans' Data from Foreign Adversaries Act of 2024," Congress.gov, March 21, 2024, <https://www.congress.gov/bills/118th-congress/house-bill/7520/all-actions>, Angelika Munger, "House Passed New Bill to Prohibit Data Brokers from Transferring Sensitive Data to Foreign Adversaries," *The National Law Review*, March 21, 2024, <https://natlawreview.com/article/house-passed-new-bill-prohibit-data-brokers-transferring-sensitive-data-foreign>.

² "United States-Mexico-Canada Agreement, Chapter 19: Digital Trade," Office of the United States Trade Representative, July 1, 2020, <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>.

attempted uses to defend a domestic law.³ Additionally, it is worth noting that the proposed JSI security exception is also useless, although it was not referenced in the hearing as an alternative means to protect our domestic policy. The draft JSI Security Exception replicates terms that WTO tribunals have ruled does not provide a defense for U.S. policies related to China and that President Trump’s USTR Lighthizer replaced in USMCA with effective language. WTO tribunals have ruled against the United States *twice* when U.S. officials raised the GATT Art. XXI Security Exception language included the draft JSI text. The WTO tribunals ruled that the WTO, not the United States, decides when there is an “emergency in international relations” that justifies use of the exception and that the U.S.-China situation does not qualify.

Hopefully this concrete example regarding the data brokers law answers some committee members’ questions about what the Biden administration meant when it said that its action of withdrawing U.S. support for four specific JSI proposals was done to protect domestic policy space. But this is not the only existing U.S. federal or state law that would conflict with the proposals from which support was withdrawn. There are other existing U.S. policies that would conflict with the proposed data flows and data storage rules. Also, numerous U.S. states’ Right to Repair laws that require consumers are provided access to source code updates, digital keys, schematics, and the like would be undermined by the “Source Code” proposal from which U.S. officials withdrew support. That term guaranteed extra secrecy protections just for source code and algorithms. Notably, already the trade secrets and other expansive existing intellectual property protections provided by the WTO and free trade agreements (FTAs) cover source code and algorithms. (Point 3 in this testimony notes what existing WTO and FTA rules *already* provide the protections some of the hearing witnesses argued were the justification for the four digital trade rules from which U.S. officials withdrew support.) Finally, a proposal on “non-discrimination”—which altered the standard language found in past U.S. pacts that forbade discriminatory treatment based on the nationality of a firm or product—would undermine various tech competition proposals before the U.S. Congress with bipartisan support. The twisted language in this proposal would make competition policies and other laws that apply equally to domestic and foreign firms and platforms an illegal trade barrier if it might have a disparate impact on a foreign firm not based on that firm’s nationality, but because of the firm’s dominance in a market. But of course, anti-monopoly policies inherently focus on market dominance. If enacted, this policy would have meant that competition policies that the U.S. Congress might enact could be applied to U.S. firms, but not to, say, a huge Chinese firm doing business here like Alibaba.

It was not only federal law that could have threatened if the digital trade proposals in question had been enacted. We recently conducted research that identified more than 100 state laws in 42 states and Washington, DC, covering Right to Repair, children’s online safety, civil liberties, artificial intelligence (AI) safety, and other measures that would conflict with the four specific proposals from which the Biden administration withdrew support.⁴

By way of background about how the proposals would have related to U.S. law, the Agreement Establishing the WTO requires: “*Each Member shall ensure the conformity of its laws, regulations and administrative procedures with its obligations as provided in the annexed Agreements.*”⁵ This means that the United States is obligated to conform its domestic law to WTO rules. The proposed

³ Daniel Rangel, “WTO General Exceptions: Trade Law’s Faulty Ivory Tower,” Public Citizen’s Global Trade Watch, February 4, 2022, 18-19, <https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/>.

⁴ “Big Tech’s ‘Digital Trade’ Agenda Threatens States’ Tech Policy Goals: Interactive State Policy Tracker,” Rethink Trade, accessed October 3, 2024, <https://rethinktrade.org/big-techs-digital-trade-agenda-threats-states-tech-policy-goals/>.

⁵ “Agreement Establishing the World Trade Organization, Art. XVI-4,” World Trade Organization, April 15, 1994, https://www.wto.org/english/docs_e/legal_e/marrakesh_decl_e.htm.

terms from which U.S. trade officials withdrew support, if ever agreed to and enacted, conflicted with and effectively would have internationally preempted U.S. federal and state law.⁶

In sum, including the wrong “digital trade” terms in agreements will undermine federal and state data privacy and security, anti-monopoly, online civil liberties, and AI policies being developed by Democrats and Republicans in Congress and state legislatures nationwide. The Biden administration’s action on digital trade at the WTO safeguards unanimously supported congressional action on data security and also protected the future ability of the U.S. Congress to enact data security and privacy provisions. As described below, the other three draft proposals from which U.S. trade officials withdrew U.S. support at JSI also conflicted with domestic policies in effect or those with bipartisan support in Congress and/or state legislatures.

2. The Biden Administration Revived Deadlocked WTO Digital Trade Talks When It Withdrew U.S. Support for Four Proposals in October 2023

Some witnesses at the hearing described the Biden administration’s actions on digital trade at the WTO inaccurately. What actually occurred was a rather routine action: On October 25, 2023, U.S. officials informed the WTO that the United States would no longer support *four specific provisions* in the draft JSI text that the Trump administration had proposed in 2019. Three other countries had supported three of these proposals for which other countries also had numerous other language proposals. This includes terms for cross border data flows, location of data storage, and source code secrecy. (Notably, most of the different versions of proposed language on data flows and storage promote free flows, but with different versions of language that typically more specifically ban specific practices, such as requiring local storage of data, requiring use of local servers, etc. and that include functioning exceptions for privacy policy.) The fourth U.S.-proposed provision, on Non-Discriminatory Treatment of Digital Products, already had been relegated to an annex of orphan ideas along with scores of pages of other proposals that had been unable to gain a single other country in support. Countries routinely withdraw or add “attributions” at the WTO, which is to say they notify those leading negotiations whether their country indicator can be listed in favor of or should be delisted from a specific proposal or draft text in a negotiation. In October 2023, U.S. officials asked to have “US” removed from four draft proposals.

Contrary to the comments of witnesses, the administration did NOT somehow remove terms from an existing WTO agreement. At issue was a draft text for talks that had been deadlocked since their 2019 start. From the beginning, numerous countries had tabled diametrically opposing language for scores of provisions and these conflicts had not been resolvable over the proceeding years of JSI negotiations.

Contrary to the comments of witnesses, the Biden administration did NOT walk away from JSI talks or end U.S. engagement in them. Indeed, U.S. officials remained engaged and, ironically, the U.S. October 2023 action and ongoing engagement moved the negotiations closer to completion. The terms from which U.S. trade officials withdrew support were never going to be included in a final deal because there were blocs of countries with diametrically opposed positions and no middle ground available after four years of discussions. Those terms have passionate support by the largest tech platforms and the business trade associations and think tanks that they fund. But most governments, including other western democracies, opposed these terms as handcuffing their domestic authority with respect to oversight of the digital economy and its impact on basic rights, including privacy, civil

⁶ Daniel Rangel and Lori Wallach, “International Preemption by ‘Trade’ Agreement: Big Tech’s Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies,” Rethink Trade, last modified March 15, 2023, <https://rethinktrade.org/reports/international-preemption-by-trade-agreement/>.

liberties and the like, and well-functioning markets.

When the U.S. government announced that it needed to reconsider its approach to the most contested digital trade topics so as to preserve policy space for the U.S. Congress and regulators, it simply underscored what had been apparent for years in Geneva at the JSI talks: There was no consensus among the participating countries about *if*—much less *how*—the WTO should address certain questions about data and algorithms. After the U.S. attributions notification in October 2023, the countries chairing the negotiations issued a new JSI text at the end of 2023 that covered the provisions on which consensus was possible. The talks seemed to have been on track for conclusion at the end of 2024. But then the countries leading the talks refused to modify the Security Exception to make it operational as U.S. officials have demanded for several years and have refused to address several specific drafting problems in a close-to-final text. As a result, quite a few countries have indicated that they cannot support the latest text until these issues are remedied, and the JSI negotiations will continue into 2025.

3. Clarifying the Protections Already Provided by WTO and Other Trade Agreement Rules and Why Adding New “Digital Trade” Rules Will Not “Fix” Problematic Conduct by Autocratic Countries

The companies that seek the certain digital trade rules seemingly to limit domestic regulation have not explained their goals as such. Rather, the firms, their trade associations, and other groups that they fund argue in favor of USMCA-style digital trade data flows and algorithm/source code special secrecy rules as critical to protecting an “open” internet and fighting against autocratic governments’ online surveillance, informational platform blocking and other abuses.

While some of the problems that they spotlight are real and serious, the sorts of digital trade rules that they propose will not provide solutions. To start with, there already are rules in effect in the WTO and other trade pacts that provide the protections that, ostensibly, the USMCA-style digital trade rules from which the United States withdrew support are intended to enact.

A witness spoke about autocratic governments blocking news media and other sites that would provide people critical information about their governments and more. But such access is a matter of information flow, which is covered by the WTO’s General Agreement on Trade in Services (GATS) Telecommunications Annex, not the data flow proposals from which U.S. officials withdrew support at the JSI. The GATS Telecommunications Annex Article 5(c) already requires companies to allow access to their telecommunications networks for free movement of information:

*5. (c) Each Member shall ensure that service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, including for intra-corporate communications of such service suppliers, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Member. Any new or amended measures of a Member significantly affecting such use shall be notified and shall be subject to consultation, in accordance with relevant provisions of the Agreement.*⁷ (emphasis added)

⁷“General Agreement on Trade in Services: Annex on Telecommunications,” World Trade Organization, accessed October 3, 2024, https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm. Definitions of the key terms are provided in Article 3: “(Definitions) For the purposes of this Annex: (a) ‘Telecommunications’ means the transmission and reception of signals by any electromagnetic means. (b) ‘Public telecommunications transport service’ means any telecommunications transport service required, explicitly or in effect, by a Member to be offered to the public generally. Such services may include, inter alia, telegraph, telephone, telex, and data transmission typically involving the real-time transmission of customer-supplied information between two or more points without any end-to-end

Another witness argued that the U.S. government withdrawal of support for the special source code and algorithm secrecy rules opened the door for China and other competitors to steal U.S. innovations. But existing World Trade Organization (WTO) obligations and many nations' domestic laws already require governments to provide copyright protections and guarantees against disclosure of companies' confidential business information, including software's source code and other algorithmic data.⁸ There is no justification for special secrecy guarantees just for digital platforms and products. U.S. law does not offer this. Rather, U.S. law provides what the WTO's Agreement on Trade-Related Aspects of Intellectual Property Article 39 on "Protection of Undisclosed Information" already requires of all WTO nations. That is 'trade secrets' protection for firms' business-confidential information and for data submitted to government authorities for regulatory purposes. (For example, the U.S. government can require a firm to provide, for instance, the formula and testing data for a drug it wants to sell in the United States, but is prohibited from sharing that data beyond the officials conducting the safety and efficacy review.)

Industry interests say the "Source Code" proposal from which U.S. officials withdrew support would stop foreign governments from passing U.S. firms' innovations to competitors. But China and other nations have spent 30 years flouting the existing WTO trade secrets rules: These countries are not going to change conduct because of new trade-pact terms on paper that say they should provide tech firms additional secrecy protections.

The actual result would be only to limit U.S. regulators and tech oversight in other countries that do adhere to the rule of law.⁹ Stronger enforcement of existing rules against Chinese or other governments passing off confidential information to business competitors of U.S. firms seems in order. However, the proposed new digital trade secrecy rule would not alter the fact that countries willing to flout the existing trade secrets rules will not suddenly change because there are more rules. But such terms would undermine the sovereignty of the U.S. Congress in deciding how it will regulate AI, ensure civil liberties in an era of pervasive facial recognition applications, and ensure state Right to Repair laws can survive. Indeed, the digital trade secrecy guarantees would bind scores of democratic countries worldwide that are considering new rules to prescreen or otherwise review the algorithms and source code running artificial intelligence applications in sensitive sectors. That industry's real goal is foreclosing AI regulation is underscored by the fact that the countries currently involved in U.S.-led trade negotiations do not have policies in place or under consideration that require government access to or transfer of source code or proprietary algorithms, according to a 2023 U.S. government review.¹⁰

change in the form or content of the customer's information. (c) 'Public telecommunications transport network' means the public telecommunications infrastructure which permits telecommunications between and among defined network termination points."

⁸ Ulla-Maija Mylly, "Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software," *IIC* 52, (2021): 1314-1337, <https://doi.org/10.1007/s40319-021-01120-3>.

⁹ It is worth noting that the USMCA "Source Code" term (Art. 19.16) replicated in the JSI proposal from which support was withdrawn has a limited exception for a "regulatory body" or a "judicial authority" to demand disclosure "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding." This exception is extremely limited: It does not allow for general pre-screenings or pre-market reviews that are needed to avoid widespread online civil liberties, competition law, and other violations. Such pre-market reviews are central to many artificial intelligence safety and oversight policies. Plus, this exception does not permit governments to require firms to provide consumers with software updates or digital keys that are necessary for consumers' Right to Repair.

¹⁰ Regarding countries involved in the Indo-Pacific Economic Framework Negotiations, see: "What Industry Identified as 'Digital Trade Barriers' in the Indo-Pacific Region as Part of the National Trade Estimate Report Process," Rethink Trade, last modified April 17, 2023, <https://rethinktrade.org/reports/ipcf-nte-digital-trade-barriers/>. Neither Kenya or Taiwan nor any Latin American or Caribbean country has imposed or is considering imposing this type of requirement according to the 2023 National Trade Estimate report. See: United States Trade Representative, "2023 National Trade Estimate Report on Foreign Trade Barriers," Office of the United States Trade Representative, March 2023, <https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf>.

4. The Biden Administration Has Broad Support for Its Approach to Digital Trade

While the lineup of the hearing certainly did not make this apparent, the Biden administration enjoys support for its digital trade policy from most¹¹ congressional Democrats,¹² some congressional Republicans, business groups,¹³ civil rights groups,¹⁴ labor¹⁵, and many other outside groups¹⁶ for ensuring that closed-door trade talks in Geneva did not force international rules that would limit what Congress decides to enact as U.S. policy or that preempts our states.

USTR had suspended negotiations on similar terms in the Indo-Pacific Economic Framework (IPEF) in spring 2023 after Democrats¹⁷ and GOP¹⁸ in Congress, digital businesses like Yelp,¹⁹ unions,²⁰ civil rights²¹ and faith groups, privacy²² and right to repair²³ advocates, and consumer groups²⁴ raised concerns.

5. The Biden Administration Digital Trade Approach Reaffirms Decades of Past U.S. Policy While the Proposals Tabled at the WTO JSI Negotiations Represented a Stark Break with Decades of U.S. Policy

As a practical matter, U.S. trade officials' actions on digital trade in 2023 *reaffirmed* longstanding

¹¹ “DeLauro Leads 87 Representatives in Letter Supporting U.S. Trade Representative Katherine Tai’s Worker-Centered Digital Trade Policy,” Office of United States Representative Rosa DeLauro, February 13, 2024, <https://delauro.house.gov/media-center/press-releases/delauro-leads-87-representatives-letter-supporting-us-trade>.

¹² “Warren, Schakowsky Lead 10 Lawmakers Commending Biden Administration for Countering Big Tech Influence in Trade Negotiations,” Office of United States Senator Elizabeth Warren, November 6, 2023, <https://www.warren.senate.gov/oversight/letters/warren-schakowsky-lead-10-lawmakers-commending-biden-administration-for-countering-big-tech-influence-in-trade-negotiations>.

¹³ “Coalition for App Fairness Applauds Biden-Harris Administration’s Withdrawal from Digital Trade Negotiations,” Coalition for App Fairness, last modified November 13, 2023, <https://appfairness.org/coalition-for-app-fairness-applauds-biden-harris-administrations-withdrawal-from-digital-trade-negotiations/>; “Yelp Letter to President Biden Re: Trade and Competition,” Yelp Inc., last modified November 8, 2023, <https://blog.yelp.com/wp-content/uploads/2024/01/Yelp-Letter-to-President-Biden.docx.pdf>.

¹⁴ “Groups Praise USTR Tai for Defending Privacy, Workers & Civil Rights in ‘Digital Trade’ Negotiations,” Trade Justice Education Fund, last modified February 2, 2024, <https://tradejusticefund.org/groups-praise-ustr-tai-for-defending-privacy-workers-civil-rights-in-digital-trade-negotiations/>; Cristiano Lima-Strong with David DiMolfetta, “Civil Rights Groups Warn Trade Talks May Hurt Efforts to Counter Discriminatory Algorithms,” *Washington Post*, May 25, 2023, <https://www.washingtonpost.com/politics/2023/05/25/musk-gives-desantis-twitter-boost-breaking-another-tech-norm/>.

¹⁵ AFL-CIO (@AFLCIO), “The Biden Administration’s decision to withdraw U.S. support for Big Tech-friendly digital trade rules at the WTO is a win for workers, consumers, and society...,” X (formerly Twitter), November 10, 2023, <https://x.com/AFLCIO/status/1722962710231482512>; “Groups Thank Biden, Tai for Course Change on ‘Digital Trade,’” Rethink Trade, last modified November 2, 2023, <https://rethinktrade.org/letters-filings/letter-to-president-biden-on-digital-trade-ipef-nov-2023/>.

¹⁶ “Groups Thank Biden, Tai.”

¹⁷ “Senator Warren, Lawmakers Reiterate Concern over Big Tech Pushing Digital Trade Rules that Conflict with Biden Competition Agenda and Pending Legislation,” Office of United States Senator Elizabeth Warren, April 21, 2023, <https://www.warren.senate.gov/oversight/letters/senator-warren-lawmakers-reiterate-concern-over-big-tech-pushing-digital-trade-rules-that-conflict-with-biden-competition-agenda-and-pending-legislation>.

¹⁸ Emily Bimbaum, “Republican Lawmakers Call for Tech Lobby Be Blocked from Indo-Pacific Trade Input,” *Bloomberg*, May 4, 2023, <https://www.bloomberg.com/news/articles/2023-05-04/gop-lawmakers-urge-denial-of-tech-lobby-indo-pacific-trade-input?ref=q0qR8k34>.

¹⁹ Cristiano Lima-Strong, “Big Tech Rivals Enter Fight over U.S. Digital Trade,” *Washington Post*, May 18, 2023, <https://www.washingtonpost.com/politics/2023/05/18/big-tech-rivals-enter-fight-over-us-digital-trade/>.

²⁰ “A Worker-Centered Digital Trade Agenda,” AFL-CIO, last modified February 7, 2023, <https://aflcio.org/worker-centered-digital-agenda>.

²¹ Lima-Strong with DiMolfetta, “Civil Rights Groups Warn Trade Talks May Hurt Efforts to Counter Discriminatory Algorithms.”

²² “Letter to President Biden: Don’t Replicate Big-Tech-Favored Terms in IPEF,” Rethink Trade, last modified March 15, 2023, <https://rethinktrade.org/letters-filings/letter-to-president-biden-dont-replicate-big-tech-favored-terms-in-ipef/>.

²³ “Letter on ‘Digital Trade’ Implications for Right to Repair,” PIRG, last modified September 12, 2023, <https://pirg.org/resources/letter-on-digital-trade-implications-for-right-to-repair/>.

²⁴ “403 Labor and Civil Society Groups Outline Shared Priorities for Indo-Pacific Trade Deal,” Citizens Trade Campaign, last modified March 2, 2023, <https://www.citizenstrade.org/ctc/blog/2023/03/02/403-labor-and-civil-society-groups-outline-shared-priorities-for-indo-pacific-trade-deal/>.

U.S. trade pact e-commerce rules. The USMCA rules that the Trump administration had proposed at the JSI were an anomaly relative to the e-commerce policies that had been included in some U.S. trade agreements since the early 2000s. These free trade agreement “E-Commerce” chapters set technical rules on online exchanges of goods and services, such as parameters for legitimate digital contracts and rules for “Paperless Trading.” The U.S. supports those rules at the JSI as well.

But what Big Tech interests have branded as “digital trade” rules and started pushing in more recent pacts is entirely different.²⁵ It focuses on controlling countries’ *domestic* agendas by restricting or altogether forbidding common policies relating to online privacy and data security, tech anti-monopoly, online civil liberties, and AI oversight even if these policies apply equally to domestic and foreign firms.

The notion repeated at the hearing that the Biden administration had moved away from a “longstanding” U.S. position is simply false. USMCA is one of the only agreements in the world with the Big Tech-favored “digital trade” provisions, which do not appear in other nations’ pacts that have digital terms or in past U.S. agreements. Indeed, USMCA is the only U.S. agreement approved by Congress that has the terms that formed the basis of the proposals from which U.S. officials withdrew support at the WTO in 2023. With respect to the USMCA, few in Congress realized that USMCA even had a “Digital Trade” chapter until it was too late to remove the terms that had never been in past U.S. trade pacts with E-Commerce chapters. (Then-Speaker Pelosi and some conservative Republican senators tried to do so when they became aware.) The past U.S. pacts with E-Commerce terms do NOT forbid governments from regulating data flows, do not provide extra secrecy guarantees for algorithms and source code beyond the trade secrets and other IP protections provided in the WTO and numerous other pacts, and do not label laws on digital antitrust that treat domestic and foreign firms the same as illegal trade barriers.

6. The Digital Trade Proposals from which U.S. Officials Withdrew Support Would Undermine Congress’ Ability to Determine U.S. Policy

To underscore the point raised above about the uselessness of the “public policy exception” that is included in one of the four proposals from which U.S. officials withdrew support, committee Republicans might be most comfortable reading USTR Lighthizer’s report on the threat to U.S. sovereignty posed by the WTO and its rulings.²⁶ With respect to whether the proposed digital trade rules could pose such threats, the strongest case is made by industry groups that have spent years criticizing privacy laws and digital competition proposals in other countries as illegal trade barriers.²⁷ This includes lobbying for U.S. trade officials to attack Australia’s News Media Bargaining Code and a similar Canadian policy that are almost identical to the proposed U.S. Journalism Competition and Preservation Act because they violate U.S.-Australia FTA or USMCA obligations, which in fact they do not. There have been similar industry attacks on Korea’s App Store policy that is very similar to the U.S. Open App Markets Act based on claims that it violates the U.S.-Korea FTA. These policies do not violate those agreements because the Korea and Australia pacts do not include the extreme terms found in the USMCA that were the basis for the proposals from which U.S. officials withdrew support at the

²⁵ David Dayen, “Big Tech Lobbyists Explain How They Took Over Washington,” *The American Prospect*, April 18, 2023, <https://prospect.org/power/2023-04-18-big-tech-lobbyists-took-over-washington/>.

²⁶ “Report on the Appellate Body of the World Trade Organization,” Office of the United States Trade Representative, February 2020, <https://ustr.gov/sites/default/files/enforcement/DS/USTR.Appellate.Body.Rpt.Feb2020.pdf>.

²⁷ Daniel Rangel, Taylor Buck, Erik Peinert, and Lori Wallach, “Digital Trade’ Doublespeak: Big Tech’s Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies,” Rethink Trade, last modified November 2, 2022, <https://rethinktrade.org/reports/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/>.

JSI. And the Canadian law does not violate USMCA because Canada negotiated a specific carveout for the applicable sector.

Yet cynically, today the same corporate lobbyists who have been using trade pact claims to attack other countries' laws that are similar to U.S. proposals with bipartisan support now are arguing there is no threat to digital regulation posed by the trade-pact digital trade rules that they seek. Thankfully, they put the original claims in writing. In a 2022 study, we documented years of written submissions related to the U.S. National Trade Estimate process where the industry interests now claiming such rules guarantee policy space argued the opposite as they urged trade challenges of numerous laws similar to those Congress seeks to enact here.²⁸

Notably, the only reason why those corporate digital policy complaints have not translated into formal trade challenges is because most agreements do not have the extreme "digital trade" rules needed to do so. This fact also highlights the irrelevance of the argument that the fact that countries worldwide are regulating the digital sphere proves that the proposals from which U.S. officials withdrew support do not pose any problem. In fact, these rules are not in place now. Very few agreements include any of the language represented in the proposed text from which U.S. officials withdrew support. That is why the proposals from which the United States withdrew support have not undermined other countries' privacy, digital anti-trust, Right to Repair and other laws – not because the dust-binned proposals are compatible with the sorts of domestic digital policies Republicans and Democrats alike in Congress and in state legislatures have enacted or are contemplating.

CONCLUSION

For generations, 1100 Longworth, the historic Ways and Means hearing room, has witnessed the Republican- and Democratic-led Ways and Means Committee express concern about Executive Branch officials disrespecting Congress's constitutional authorities—over trade, over law-writing, and more. The September 2024 digital trade hearing seemed an anomaly to this rare matter of bipartisan consensus. Instead of thanking U.S. trade officials for preserving Congress's authority to determine key domestic policies and derailing what would have been broad international preemption of Congress's and U.S. state legislatures' policy space via "digital trade" agreement, some committee members were highly critical of the administration. While certainly there are disagreements within Congress and state legislatures about *how* to best ensure Americans' privacy online, data security, fair digital markets, civil liberties in a digital age, AI oversight, and more, certainly such U.S. policies should be determined through democratic processes at home, not imposed via WTO or other trade agreement rules that cannot be altered by one word but for consensus of every signatory country.

²⁸ Rangel et al., "'Digital Trade' Doublespeak."

Congress of the United States

Washington, DC 20515

February 12, 2024

The Honorable Joseph R. Biden, Jr.
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear Mr. President:

We are writing to commend Ambassador Katherine Tai's approach to developing and implementing your Administration's inclusive and worker-centered trade policy, especially on matters related to the digital economy.

We appreciate greatly Ambassador Tai's acknowledgement that trade officials should not attempt to preempt Congress on domestic policy through trade negotiations. It is a credit to your presidency that Ambassador Tai is proceeding in a manner that respects Congress' role in setting domestic policy and that honors your digital competition, privacy, and artificial intelligence (AI) oversight goals, which we also support. For instance, during the Aspen Security Forum Ambassador Tai noted that your Administration has deliberately examined the position taken by the previous Administration on certain digital trade matters to assess whether it aligns with your Administration's regulatory approach, the debates in Congress, and the broader public conversation regarding these issues. We agree with Ambassador Tai's assessment that getting ahead of the domestic debates on these issues would be malpractice.

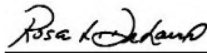
Your Administration's approach contrasts favorably with the previous Administration, which used trade agreements to derail domestic policy debates. Specifically, the Trump Administration inserted several "digital trade" provisions favored by Big Tech interests into the U.S.-Mexico-Canada Agreement. These provisions, which had not been in past U.S. trade agreements, were designed to limit the regulation of domestic online privacy and data security matters, gig worker protection, AI oversight, tech anti-monopoly, and other important policies.

We appreciate that Ambassador Tai has made clear at the World Trade Organization and in the Indo-Pacific Economic Framework negotiations that your Administration will not allow these Trump-era rules to derail the debate in the U.S. Congress on crafting rules for the digital economy. As you may know, dozens of bills have been introduced so far in the 118th Congress, many of them with bipartisan support, that would establish online privacy, data security, online civil rights and liberties, AI oversight, and anti-trust policies. We are concerned that trade negotiations on certain digital rules could get ahead of Congress' domestic policymaking.

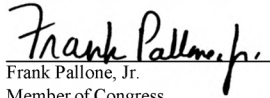
We also want to commend you for Ambassador Tai's strong and strategic approach to trade policy with countries who are not our allies, such as China and Russia. Ambassador Tai reasserted our rights to limit the flow of Americans' data to such countries by withdrawing U.S. support for Trump-era WTO proposals that granted data brokers and digital platforms all but total control of Americans' data. These proposed provisions would have constrained Congress and U.S. government agencies from restricting the flows of Americans' data for national security or privacy reasons.

We look forward to working with your Administration to ensure that any trade rules covering digital policy provide Congress with the policy space needed to safeguard the interests of American workers, entrepreneurs, smaller businesses, and consumers.

Sincerely,



Rosa L. DeLauro
Member of Congress



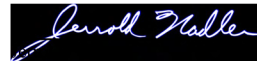
Frank Pallone, Jr.
Member of Congress



Member of Congress



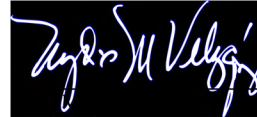
Maxine Waters
Member of Congress



Member of Congress



Member of Congress



Member of Congress



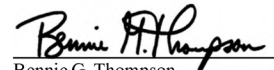
James P. McGovern
Member of Congress



Mark Takano
Member of Congress



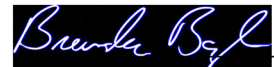
Member of Congress



Bennie G. Thompson
Member of Congress




Joseph D. Morelle
Member of Congress



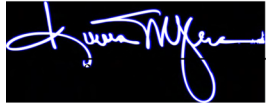
Brendan F. Boyle
Member of Congress



Member of Congress



Donald Norcross
Member of Congress



Bonnie Watson Coleman
Member of Congress



Jil Tokuda
Member of Congress



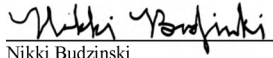
Paul D. Tonko
Member of Congress



Donald M. Rayne, Jr.
Member of Congress



Iman Omar
Member of Congress



Nikki Budzinski
Member of Congress



Linda T. Sanchez
Member of Congress



Patrick K. Ryan
Member of Congress



Betty McCollum
Member of Congress



Joe Courtney
Member of Congress




Adam B. Schiff
Member of Congress



Chellie Pingree
Member of Congress



Jon Jost
Member of Congress




Pramila Jayapal
Member of Congress



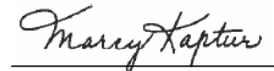
Jan Schakowsky
Member of Congress



Veronica Escobar
Member of Congress



Chris DeFazio
Member of Congress




Marcy Kaptur
Member of Congress



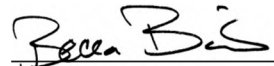
Greg Casar
Member of Congress



Eleanor Holmes Norton
Member of Congress



Barbara Lee
Member of Congress



Becca Balint
Member of Congress



Ro Khanna
Member of Congress



Jamaal Bowman, Ed.D.
Member of Congress



Katie Porter
Member of Congress



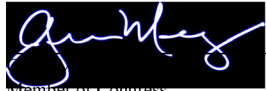
Stephen F. Lynch
Member of Congress



Member of Congress



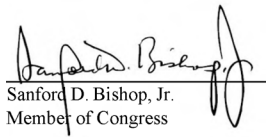
Member of Congress



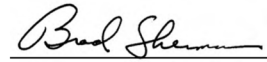
Member of Congress



Frederica S. Wilson
Member of Congress



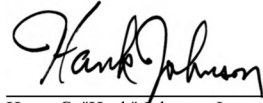
Sanford D. Bishop, Jr.
Member of Congress



Brad Sherman
Member of Congress



Lori Trahan
Member of Congress



Henry C. "Hank" Johnson, Jr.
Member of Congress



John Garamendi
Member of Congress



Member of Congress



Member of Congress



Member of Congress



Member of Congress



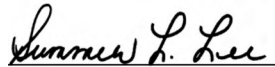
Member of Congress

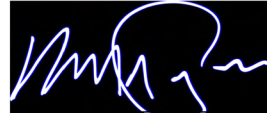


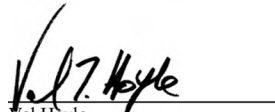
Rashida Tlaib
Member of Congress

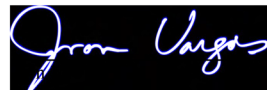


Member of Congress

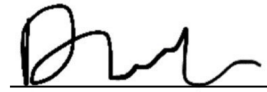

Summer Lee
Member of Congress


Mark Pocan
Member of Congress


Val Hoyle
Member of Congress


Jon Unger
Member of Congress


Mark DeSaulnier
Member of Congress

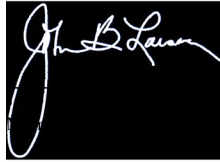

Dan Goldman
Member of Congress


Cori Bush
Member of Congress


Steve Cohen
Member of Congress


Alma S. Adams, Ph.D.
Member of Congress


Member of Congress



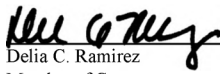
André Carson
Member of Congress



Member of Congress



Member of Congress



Delia C. Ramirez
Member of Congress



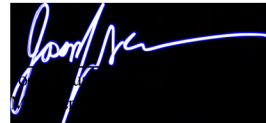
Lloyd Doggett
Member of Congress



Member of Congress



Valerie P. Foushee
Member of Congress





JOAQUIN CASTRO



Ayanna Pressley
Member of Congress



Sheila Cherfilus-McCormick
Member of Congress



Sheri Jackson Lee
Member of Congress



Salud Carbajal
Member of Congress



Salud Carbajal
Member of Congress



Member of Congress



Robin Kelly



C. A. Dutch Ruppertsberger
Member of Congress



PO Box 77043
 Washington, DC 20013
info@tradejusticefund.org
 202-494-8826

Chairman Jason Smith and Trade Subcommittee Chairman Adrian Smith
 Committee on Ways & Means
 1139 Longworth House Office Building
 Washington, DC 20515-6348

VIA EMAIL

Re: Written Testimony for the Subcommittee on Trade's September 20th Hearing on Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules

September 23, 2024

Dear Chairman Smith and Trade Subcommittee Chairman Smith:

Thank you for the opportunity to submit written testimony in the Ways & Means Subcommittee on Trade's hearing on the importance of U.S. leadership in establishing and enforcing strong digital trade rules. These comments are submitted on behalf of the Trade Justice Education Fund, a nonprofit organization working to expand awareness about the worker rights, environmental, consumer and public health implications of U.S. trade policy.

Our organization commends U.S. Trade Representative (USTR) Katherine Tai for leading the update of "digital trade" rules to provide the policy space necessary for Congress and government actors to enact urgently-needed policies on Big Tech competition, gig worker rights, online consumer privacy, data security and artificial intelligence (AI) accountability measures.

We particularly appreciated USTR's action in late 2023 to withdraw U.S. support for extreme "digital trade" proposals at the World Trade Organization (WTO), which we view as an important first step to ensuring that Big Tech interests cannot commandeer trade negotiations to undermine the important platform accountability policies being developed by Congress and others. The provisions from which USTR withdrew U.S. support do not appear in most other countries' agreements nor in most U.S. free trade agreements that have had E-Commerce chapters over the past two decades.

These harmful, but now thankfully withdrawn, provisions include:

- **Two provisions that guarantee tech firms nearly absolute control of our personal data. They ban government policies to protect our privacy and ensure data security, such as proposals to prevent Americans' data going to bad actors overseas.** Other WTO members support a more balanced version of "Data Flows" and "Location of Computing Facilities" rules that preserves governments' rights to regulate;

for a just and sustainable global economy

- **A provision that provides tech firms special secrecy guarantees that would thwart government review of algorithms and AI to curb racial discrimination, gender discrimination, labor violations and more, while also undermining the “Right to Repair” that family farm organizations and others have acknowledged as vital.** The WTO already requires countries to provide trade secrets protection for business-confidential information. This “Source Code” rule would forbid meaningful government oversight altogether. Our trade agreements should not provide special secrecy rights to digital firms to evade government oversight; and
- **A provision that undermines antitrust and competition policy and enforcement of labor, health or other laws in the digital sphere that may affect larger firms more.** This rule twists a trade principle called non-discrimination to make facially neutral laws that may have a disparate impact on foreign firms an illegal trade barrier.

Unlike these dangerous proposals, strong digital trade rules would instead promote worker rights, consumer privacy, civil rights and data security goals. Good rules for the global economy allow governments to retain policy space to regulate, while in the digital sphere also promoting data flows and disciplining actual discrimination.

Even if Big Tech lobbyists may be upset that their efforts to quietly preempt online privacy and antitrust policies, gig worker protections and AI oversight policies are derailed, most Americans would be thrilled to learn their government is rejecting Big Tech demands in this area. To that point, I am attaching the text of a letter our organization sent to the President in November 2021 on behalf of more than 50 digital privacy, consumer, human rights, labor, faith and other civil society organizations calling for “digital trade” rules to uplift workers, ensure racial justice, protect consumers and enable fair competition. I ask that you please add that letter and this note into the public record for your hearing.

Sincerely,

Arthur Stamoulis, Executive Director
TRADE JUSTICE EDUCATION FUND

The Honorable Joseph R. Biden, Jr.
 President of the United States
 The White House
 1600 Pennsylvania Ave NW
 Washington, DC 20500

November 2, 2021

Dear President Biden:

Our organizations appreciate your administration's focus on developing new, people-centered trade policies and agreements that advance worker rights, racial equity and consumer safeguards here and across borders. We are excited to work with you and U.S. Trade Representative Katherine Tai to fulfill that vision. We write today to express our interest and desire to ensure trade policies of any stripe, including recent discussions about "digital trade" policy, uplift workers, ensure racial justice, protect consumers and enable fair competition.

Many supporters of the status quo trade regime are pushing policies through the "digital trade" framework aimed at helping massive global retail, advertising, transportation, hotel and other businesses evade regulation and oversight. These proposals are not focused on remedying actual problems related to the online sale of imported goods, such as tariff evasion and product safety. Instead, Big Tech interests have promoted binding international rules to limit governments worldwide from regulating online platforms in the interest of workers, consumers or smaller business competitors.

Misbranding constraints on government regulatory authority as "e-commerce" or "digital trade" agreements has helped them to evade scrutiny and quietly undermine certain worker protections, policies that constrain entities' size or market power and promote fair competition, and civil rights, privacy and liability policies being considered by your administration, many in Congress from both parties and other governments worldwide. By hijacking common trade-pact concepts, such as "non-discrimination," the largest digital firms seek to secure their monopolistic dominance by labeling as illegal trade barriers countries' labor, competition and other domestic policies of general application simply because such policies may have greater impact on the largest firms because of the firms' size.

At a time when the United States and the world are grappling with how to best regulate Big Tech in areas as disparate as gig economy worker protections, discrimination and algorithm transparency, competition policy and anti-trust, corporate liability, and consumer privacy, we must not establish "trade" rules that restrict or dissuade countries from regulating digital entities or that impose or lock in retrograde domestic digital governance policies.

Harmful "digital trade" proposals include those that serve to:

- ***Hurt working people by prioritizing corporate interests ahead of labor rights and the protection of gig workers.*** No trade or other international commercial agreement should limit countries' policies that condition permission for an entity to operate on compliance with

labor, health and safety, civil rights, competition, consumer and other policies that apply across an economy or to a sector. Requiring large ride-sharing companies, for instance, to meet driver hours-of-service-rules or to contribute to social security for drivers or requiring buildings of short stay guest units booked online to meet worker and consumer safety rules, must never be characterized as a “trade barrier” nor as “censorship” if failure to comply means an end to operating permissions. Trade and commercial agreements must not be allowed to become Trojan Horse tools for attacking, weakening, preventing or dismantling labor or other public interest policies. Instead, all trade agreements should be structured to raise the floor to help ensure that all workers’ rights are protected, regardless of country.

- ***Hide the discriminatory effects of source code and algorithms through “trade secrets” protections.*** Governments increasingly are turning to private corporations for aid with “predictive policing” and other surveillance, law enforcement and security functions. And, every-day decisions made by artificial intelligence components of online platforms increasingly affect which individuals and communities are offered access to public and private services ranging from home loans to job postings to medical treatments. International commercial agreements cannot repurpose “trade secrets” protection rules or establish other “digital trade” rules that limit the ability of regulators, academics, civil society and the public to access and review the underlying technology for discriminatory practices deserving of scrutiny, criticism and correction. Similarly, “digital trade” rules cannot establish rights and protections for online entities that allow them to evade liability for discriminatory conduct and civil rights violations.
- ***Undermine consumer privacy and data security by prohibiting limits on data flows or rules on the location of computing facilities.*** Peoples’ every move on the internet and via cell phones is increasingly tracked, stored, bought and sold — as are interactions with the growing “internet of things,” that many people may not even be aware are tracking them nor from which they have a feasible way to opt out. Trade pacts must not restrict governments from acting on the public’s behalf in establishing rules regarding under what conditions individuals’ personal data may be collected, where it can be processed or transmitted, and how or where it is stored.
- ***Shield Big Tech firms from corporate accountability via overly broad content liability waivers.*** How to address the ways in which certain online business practices, algorithms and moderation stoke racial and ethnic violence and contribute to other anti-social behavior is a hotly debated topic. While there is no consensus on policy solutions, what is absolutely true is that this rapidly evolving area of public policy must not be restrained via trade agreements. Using trade pacts to prevent signatory countries from determining the best ways to protect the public interest online is unacceptable.
- ***Protect Big Tech monopolies and promote further consolidation by banning limits on size, services offered or break-ups.*** As corporations and conglomerates exert increasing control over important social functions, governments must be able to combat anti-competitive business practices, place limits upon corporate mergers and break up monopolies where warranted. Digital trade rules must not include terms that forbid countries from establishing

or maintaining policies that limit the size or range of services offered by companies, limit the legal structures under which they may be required to operate, nor otherwise restrict the regulation or break-up of Big Tech monopolies.

Certain terms of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Digital Economic Partnership Agreement (DEPA) and leaked text from the World Trade Organization (WTO)-adjacent “e-commerce” talks are problematic in many of these areas. The administration must avoid any negotiations or agreements that would replicate troubling anti-worker, anti-consumer and anti-democratic policies.

As governments worldwide struggle to address fundamental issues relating to digital governance, these important policy debates and decisions that will shape every facet of our lives must not be constrained, undermined or preempted via “trade” pacts or policies. We appreciate the administration’s forward-thinking approach on the need to refocus international trade policy beyond just corporate interests, and we look forward to working with you to set appropriate trade agreement priorities.

Sincerely,

Trade Justice Education Fund
 American Economic Liberties Project
 American Family Voices
 Americans for Democratic Action
 Asian Pacific American Labor Alliance, AFL-CIO
 Association of Western Pulp & Paper Workers Union
 Center for Digital Democracy
 Citizens Trade Campaign
 Coalition of Labor Union Women
 Codepink
 Color of Change
 Communications Workers of America (CWA)
 Consumer Action
 Consumer Federation of America
 Council on American-Islamic Relations (CAIR)
 Defending Rights & Dissent
 Demand Progress Education Fund
 Demos
 Electronic Privacy Information Center (EPIC)
 Encode Justice
 Franciscan Action Network
 Global Exchange
 Government Information Watch
 Hip Hop Caucus
 Institute for Local Self-Reliance
 Institute for Policy Studies - Global Economy Project
 Jobs with Justice

Justice is Global
Media Alliance
National Association of Consumer Advocates
National Consumers League
National Organization for Women
National Workrights Institute
Network Lobby for Catholic Social Justice
Open MIC (Open Media and Information Companies Initiative)
Other98
Our Revolution
Partners for Dignity & Rights
People's Parity Project
Pride at Work
Progressive Change Institute
Public Citizen
Revolving Door Project
Service Employees International Union (SEIU)
Social Security Works
SumOfUs
The United Methodist Church - General Board of Church and Society
Transport Workers Union of America
U.S. PIRG
UNITE HERE
United Steelworkers
US Human Rights Network
Win Without War

CC: Secretary of State Anthony Blinken
Bureau of Consumer Financial Protection Director Rohit Chopra
Attorney General Merrick Garland
Federal Trade Commission Chair Lina Khan
Secretary of Commerce Gina Raimondo
Council of Economic Advisers Chair Dr. Cecilia Rouse
National Security Advisor Jake Sullivan
United States Trade Representative Katherine Tai
Secretary of Labor Marty Walsh



Engine Advocacy
700 Pennsylvania Ave SE
Washington, D.C. 20003

October 2, 2024

House Committee on Ways and Means
Longworth House Office Bldg. Rm. 1139
Washington, D.C. 20515

VIA EMAIL

Statement of Engine Advocacy re: Hearing on Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules Held September 20, 2024

Dear Chairman Smith, Ranking Member Blumenauer, and Honorable Members of the House Ways and Means subcommittee on trade:

We write to thank you for the September 20th hearing regarding the U.S. approach to digital trade. Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship. Lowering barriers to trade unlocks markets for U.S. startups to expand, compete, and find success and is a vital part of promoting domestic technology entrepreneurship. Recent backsliding on longstanding digital trade priorities threatens to raise barriers to global success for U.S. startups, and this hearing is a good step toward correcting that mistake.

Engine has regularly engaged the committee to highlight how startups rely on smart digital trade policy to keep barriers low and help them reach markets around the world. Barriers encountered by startups dictate the markets where they can reasonably enter, create additional costs that detract from investments in R&D and job creation, and hamper U.S. economic growth by limiting the flow of goods and services across borders. Engine and over 40 startups, investors, and other support organizations earlier this year urged you and colleagues across government to pursue policies to support startup success:¹

¹ See *Open letter to U.S. Trade Policymakers*, (Feb. 7, 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65c3906e36cbbb45ba281205/1707315310372/Startup+Digital+Trade+Open+Letter.pdf>

- Enable cross-border data flows and oppose local storage mandates;
- Foster innovation and regulatory consistency;
- Avoid technology-specific levies and prohibit duties on digital transmissions; and
- Streamline trading processes and support access to resources and digital tools.

We are pleased you heard from the founder of one of those startups at the hearing, Dr. Olivia Walch, cofounder and CEO of Arcascope.² Her testimony highlights the importance of a strong, proactive digital trade agenda to the success of U.S. small businesses. Dr. Walch highlighted components of this agenda: opposing “rules like tariffs on digital goods, mandatory data localization, or forced source code disclosure.” Allowing digital trade barriers to take root will lock out U.S. startups, but “does not mean innovation [...] won’t happen,” Dr. Walch underscored, it “means a non-U.S. competitor or someone better-funded and with more legal resources” will benefit instead.

These barriers must be addressed, but how we address them matters. Pursuing measures that create barriers to trade in their own right—such as tariffs or site-blocking³—in response to unfair trade practices is the wrong approach, because they will harm U.S. startups and consumers. Instead, policymakers must engage countries directly and through fora that enshrine gold-standard digital trade provisions. The U.S.-Japan digital agreement and USMCA are examples of this success. The Joint Statement Initiative on E-Commerce and the Indo-Pacific Economic Framework trade chapter negotiations were other recent opportunities that the administration missed due to their misguided new direction on digital trade.

U.S. startups need strong digital trade policy implemented by policymakers that will fight for their interests on the global stage. Many of the policies needed to support startups are those that the U.S. Trade Representative is actively backing away from. We urge you and your colleagues to use what you learned at this hearing to implore Ambassador Tai’s agency to change course. It is imperative that the U.S. pursues a strong digital trade policy agenda that ensures U.S. startups can thrive and remain global leaders in innovation.

Sincerely,
Engine

Engine Advocacy
700 Pennsylvania Ave. SE

² *Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules: Hearing before the U.S. House Ways & Means Subcomm. on Trade*, 118th Congress (2024) (Testimony of Olivia Walch), <https://waysandmeans.house.gov/wp-content/uploads/2024/09/Walch-Testimony.pdf>

³ Site blocking was cited as a remedy for copyright violations at the hearing, but that approach is akin to using a backhoe to weed a flower garden—U.S. content hosting startups are likely to be collateral damage (see, e.g., Abby Rives, *Copyright Law & Startup Innovation: Policies That Matter and Where They May be Headed*, Engine (Jan. 19, 2022), <https://engineadvocacyfoundation.medium.com/copyright-law-startup-innovation-policies-that-matter-and-where-they-may-be-headed-dea034904e25>). Further, that adopts a problematic censorial playbook from our adversaries, even if the intentions are more noble—fighting fire with fire leads to more fire.

Washington, D.C. 20003

