S. HRG. 117–879

OPPORTUNITIES AND CHALLENGES FOR TRADE POLICY IN THE DIGITAL ECONOMY

HEARING

BEFORE THE

SUBCOMMITTEE ON INTERNATIONAL TRADE, CUSTOMS, AND GLOBAL COMPETITIVENESS

OF THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

NOVEMBER 30, 2022

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

56–373—PDF WASHINGTON : 2024

COMMITTEE ON FINANCE

RON WYDEN, Oregon, *Chairman*

DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, JR., Pennsylvania
MARK R. WARNER, Virginia
SHELDON WHITEHOUSE, Rhode Island
MAGGIE HASSAN, New Hampshire
CATHERINE CORTEZ MASTO, Nevada
ELIZABETH WARREN, Massachusetts

MIKE CRAPO, Idaho
CHUCK GRASSLEY, Iowa
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
TIM SCOTT, South Carolina
BILL CASSIDY, Louisiana
JAMES LANKFORD, Oklahoma
STEVE DAINES, Montana
TODD YOUNG, Indiana
BEN SASSE, Nebraska
JOHN BARRASSO, Wyoming

JOSHUA SHEINKMAN, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

SUBCOMMITTEE ON INTERNATIONAL TRADE, CUSTOMS, AND GLOBAL COMPETITIVENESS

THOMAS R. CARPER, Delaware, *Chairman*

RON WYDEN, Oregon
DEBBIE STABENOW, Michigan
ROBERT MENENDEZ, New Jersey
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, JR., Pennsylvania
MARK R. WARNER, Virginia
CATHERINE CORTEZ MASTO, Nevada

JOHN CORNYN, Texas
CHUCK GRASSLEY, Iowa
JOHN THUNE, South Dakota
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
TIM SCOTT, South Carolina
STEVE DAINES, Montana
TODD YOUNG, Indiana
BEN SASSE, Nebraska
JOHN BARRASSO, Wyoming

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATIONS

OPPORTUNITIES AND CHALLENGES FOR TRADE POLICY IN THE DIGITAL ECONOMY

WEDNESDAY, NOVEMBER 30, 2022

U.S. SENATE,
SUBCOMMITTEE ON INTERNATIONAL TRADE,
CUSTOMS, AND GLOBAL COMPETITIVENESS,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 3:03 p.m., in Room SD–215, Dirksen Senate Office Building, Hon. Thomas R. Carper (chairman of the subcommittee) presiding.

Present: Senators Wyden, Casey, Cortez Masto, Warren, Grassley, Cornyn, and Young.

Also present: Democratic staff: Evan Giesemann, Staff Director, Subcommittee on International Trade, Customs, and Global Competitiveness; Andrew Smith, Legislative Aid for Senator Carper; and Daniel Kim, Trade Fellow for Senator Carper. Republican staff: Andrew Cooper, Legislative Assistant for Senator Cornyn.

OPENING STATEMENT OF HON. THOMAS R. CARPER, A U.S. SENATOR FROM DELAWARE, CHAIRMAN, SUBCOMMITTEE ON INTERNATIONAL TRADE, CUSTOMS, AND GLOBAL COMPETITIVENESS, COMMITTEE ON FINANCE

Senator CARPER. It looks like there is standing room only. I am delighted to welcome you all here today. It is my pleasure to sit next to Senator Cornyn, a good friend and a wonderful colleague.

I will call this hearing to order. This is a subcommittee of the Senate Finance Committee, and our focus is international trade; it is Customs; it is global competitiveness as well. And we thank our witnesses who have joined us. We have four witnesses who have joined us today, and I want to say a special "thank you" to our subcommittee's ranking member—not just Senator Cornyn but also his staff and our staff and others who have worked with him on both sides of the aisle to plan this important hearing on digital trade.

Today's hearing will offer an opportunity for us to answer not one, not two, but three central questions. The first is—and this is my favorite question—what is digital trade, anyway? I remember, Senator Cornyn, many years ago when I was, I think, chairman of a subcommittee on, I want to say, Banking, and people were starting to talk about cryptocurrency and this and that, and I didn't understand it, and my staff did not understand it, and neither did our colleagues understand it. This was at least a dozen years ago. So we said, "Why don't we hold a hearing?" And so, we held a hearing

on it. And when staff said, "Why are you doing it this way?" we said, "We just do not understand it."

At the end of the hearing, they said, "Well, do you understand it now?" Not really. And there are some people who do not understand a whole lot about digital trade, why it is important, what it means.

So the first question we are going to answer here today—for folks who might be joining us, near or far, the first question is, what is digital trade, anyway? The second question is, why is it important to our country? Why is it important to Americans as well? And finally, how can we work with our allies, with other trading partners in order to strengthen our ever-changing digital economy?

Today's hearing will also be the first Senate hearing in this Congress, I think, to specifically explore the importance of digital trade. And then we can take this dedicated time in a bipartisan way—that is the way Senator Cornyn and I like to work—to dive into what I think is a critical and ever-important issue with leading experts across our Nation.

When I first started learning about digital trade, I quickly discovered it is necessary for us to better understand and appreciate how digital technology and the Internet have transformed our economy.

I will take a couple of moments to talk about this through an example. I love examples. I like to explain concepts with stories, and we are going to try to do that today—and we will see how it works. But we will provide an example, and we are going to show you something that we have all come to know well, and that is smartphones, smartphones. And let me see if I have mine. I do. And my guess is, for everybody in this room, I could ask you to show us your smartphone. If you have a smartphone, why don't you just hold it up if you have one with you. This is good. Almost all of us—this one lady back here does not have a smartphone. We will have to get her one. But smartphones are everywhere in our society. They have them in prisons for people who should not have them, and that is a story for another day. It is not in every prison that that happens, but it is certainly a concern when it does.

But nearly everyone I know, and probably everyone that you all know, has one. It is almost impossible to imagine our lives today without them. We use them for just about everything, from checking work emails, to logging into a Zoom meeting, to purchasing goods from halfway around the world. Whether it happens to be booking a hotel in Dover, DE, or Dover, England, smartphones have made our lives more accessible for just about everything.

These are just a few examples in our daily lives that show how digital connectivity can make it easier, faster, less expensive to trade goods and services across our globe. And this is all made possible because the Internet has made it easier for us to share information and data without geographic barriers.

Without these tangible barriers, digital innovation has revolutionized nearly every industry across our country and our economy, ranging from manufacturing to agriculture to financial services to e-commerce—you name it. As a result, trading goods and services, with a lot of help from the Internet, has exploded in recent years.

Just look at the numbers from 2005 to 2019. Real value added for the U.S. digital economy grew at an annual rate of more than 5 percent per year, outpacing the 2-percent growth in the overall economy during those same years. And the pandemic has spurred digital growth even more, with people staying home and turning to the Internet to access medical services, to stream their favorite movies, or book their next vacation in the First State, or in the Lone Star State, or around the globe.

And this growth is not just benefiting consumers, it is also spurring job creation and enabling small businesses to thrive. The digital economy's small business that sells jewelry in Delaware, or Texas, or some other place can now sell the products just about anywhere in the world with ease.

However, it is critical that as we examine the importance of digital trade for our economies, we must also acknowledge how digital technologies affect our national security. Right now, we are witnessing a global battle over the values that govern the digital economy. Foreign adversaries like China are using digital technologies to advance authoritarianism and crack down on freedom of speech and human rights. They are working overtime to shape the digital economy in a way that threatens our democratic values and jeopardizes our national security.

Yet, as Albert Einstein once said—in fact, he used to say this not just once, but a lot—he used to say, "In adversity lies opportunity." I say that a lot too. I always give him credit, but I think that is a great truth. It guides me in my life, and I suspect Senator Cornyn and a whole lot of other people in this room as well.

That is exactly what we have before us today: a real opportunity to set the rules for digital trade that reflect our values. Those words were true then, "in adversity lies opportunity," and they are even truer today.

So far, the U.S. has taken a leadership role through negotiating ambitious digital rules in the USMCA agreement we have with Canada and Mexico—we used to call it NAFTA—and through digital trade, through cooperation with Japan. But that is not enough. Our work cannot stop there.

That is why this past year my staff and I have worked closely with one of our colleagues from the other side of the aisle—Senator Young and his staff and other members of this committee—to introduce a bipartisan, bicameral resolution advocating for the United States to work with our allies across the globe to establish forward-looking digital trade policies.

I am also eager to work with the U.S. Trade Representative, Katherine Tai, and the Biden administration to make progress on these important issues as they negotiate something called the Indo-Pacific Economic Framework and other economic engagements relating to digital trade.

So today, I look forward to hearing from our esteemed panel of witnesses to pull back the curtain on the importance of digital trade and how we can work with our Allies in this country, but especially outside of this country, to advance thoughtful digital trade policies.

With that, I am happy to turn it over to my wing man on this committee and others, Senator Cornyn. Thank you.

[The prepared statement of Senator Carper appears in the appendix.]

OPENING STATEMENT OF HON. JOHN CORNYN, A U.S. SENATOR FROM TEXAS

Senator CORNYN. Thank you, Mr. Chairman, for organizing this hearing. And it has been a pleasure, as always, working with your staff. And thanks to all of our witnesses for being here and sharing their expertise and knowledge.

I like the three questions that you plan to ask and have teed up here. This subcommittee has consistently focused on the threat that China poses to our national security through its weaponization of trade, contrary to the international rules-based system that we thought they were joining when they became part of the WTO.

On that note, I want to express my concerns with regard to reports that our allies in Europe may retaliate for provisions of the recently passed Inflation Reduction Act, in the face of existential challenges posed by the Chinese Communist Party and its allies in the Russian Federation. A strong relationship with our partners in Europe is more important than ever.

Unfortunately, legislation passed on a purely party-line vote like the Inflation Reduction Act has moved us in the wrong direction. I hope the administration will work to limit the trade ramifications from this bill with regard to Europe and our other Allies.

We all know that the results of protectionism helped in the past to put us into the Great Depression nearly a century ago, and we simply cannot afford to repeat it or get anywhere near it.

On this subcommittee, we have advocated for the U.S. to join the CPTPP. It was a mistake for us to walk away in the first place. I was with Senator Hagerty, the former Ambassador to Japan, now a member of the U.S. Senate, and Senator Cardin, a colleague on the Finance Committee, in Japan recently. Every single meeting we had with our Japanese Government counterparts, they mentioned the TPP. And Senator Carper and I have written and spoken together on what a mistake it was for us to walk away from that. And my hope would be that at some point we would get back in the game in Asia with the CPTPP——

Senator CARPER. Would my colleague yield for just a moment? Self-inflicted wound.

Senator CORNYN. Yes.

Senator CARPER. That's what I discovered. I'm sorry. Thank you.

Senator CORNYN. Unfortunately, so far the Biden administration has refused to reopen negotiations on that agreement, so we need to look to sectoral-specific free trade agreements focused, for example, on digital trade, which is also part of the conversation we had with Ambassador Emanuel in Japan when we were there.

As each of our colleagues know, free trade agreements passed through Congress are insulated from domestic political pressure. They provide long-term certainty for our businesses and reinforce the key economic relationships that we have with our friends and allies.

We have also focused on China's use of censorship as a barrier, to digital trade in particular. We see today how China is weap-

onizing its digital infrastructure against its own citizens for simply protesting in the streets.

One of the first tasks we should explore is how to define "digital trade," which is what Chairman Carper—the question he raised first, and appropriately so. For everything digital or virtual, from the cloud to artificial intelligence, there is obviously an underlying physical element. For digital trade, that medium is semiconductors.

So maybe we should start by using that physical apparatus as a starting point for our discussions.

The second area we should explore is how digital trade agreements help to solidify our relationship with our friends and allies against the threat posed by the Chinese Communist Party. So, I believe any digital trade agreement with our allies and partners should include provisions that incorporate disciplines on semiconductors as part of it. That includes things like coordination of semiconductor incentives, harmonization of our export controls with regard to China, and supply chain resiliency.

Finally, and most importantly, we should find common areas of agreement amongst all stakeholders, to include business, labor, and national security. That includes topics like preventing data localization and enforced technology transfers. We should have free and open digital trade facilitation with clear rules of the road.

For example, we should not be taxing electronic transmissions between our borders, or forcing data centers to be located in one nation or another. As with all issues pertaining to China, that will require a fair amount of discussion and debate, and even compromise.

So, I look forward to hearing from our witnesses today who represent a facet of each of those. I would like to welcome Mr. Feith for the national security perspective, Mr. Woodall for the labor community, Ms. Bliss from industry, and Dr. Meltzer from the think tank community that is important to give us the intellectual firepower we need to make good decisions here in Congress.

So, thank you all for being here today, and I look forward to hearing from you.

[The prepared statement of Senator Cornyn appears in the appendix.]

Senator CARPER. Thank you, John.

I would introduce as our first witness Christine Bliss, who is the president of the Coalition of Services Industries. I always like introducing the president. My wife will say to me when I get home tonight, she will say, "Who did you meet with today?" And I will say, "Well, the president." And she will say, "In what capacity?" "She was a witness before our committee." She will say, "You mean the Vice President?" "No, no, the president."

But anyway, Madam President, we are glad that you are here and your colleagues with you. You are actually the president of the Coalition of Services Industries, I am told. And the Coalition for Services Industries represents the interests of the American services economy, which employs over 75 percent of the American workforce and generates some three-quarters of national economic output. That probably would surprise a lot of people.

Previously Ms. Bliss served as the Assistant U.S. Trade Representative for Services, Investment, Telecommunications, and E-

Commerce. She also served in numerous roles in the World Trade Organization, including the lead negotiator in the DOHA services negotiation.

Ms. Bliss, you have the floor. Welcome. Thank you for joining us.

STATEMENT OF CHRISTINE BLISS, PRESIDENT, COALITION OF SERVICES INDUSTRIES (CSI), WASHINGTON, DC

Ms. BLISS. Thanks very much, Mr. Chairman. And I also appreciate the participation and comments from Ranking Member Cornyn.

I appreciate the opportunity to appear before you today and be part of this distinguished panel of witnesses. I am Christine Bliss, the president of the Coalition of Services Industries, a nonprofit association representing U.S. firms on services and digital trade issues.

Our members include distribution, logistics, financial services, professional services, and IT services companies, including manufacturers of consumer technology, telecommunications equipment, and health and nutrition products. Our members operate in all 50 States and over 200 countries, and represent both large, medium, and small firms.

The digital economy is not just about benefits to the information technology sector. And I think too often that narrow view, and maybe misunderstanding, is out there. So hopefully we can correct that. The digital economy is essential to companies, both large and small, and economy-wide, including manufacturing—and I think, as you mentioned in your opening remarks, agriculture, health, education, environment, transportation, logistics, communication, finance, distribution, media, and entertainment. And it is a major source of existing and future jobs.

To ensure that all Americans, including more workers, small businesses, and communities enjoy the benefits of digital trade, the U.S. must address growing digital protectionism abroad through high-ambition trade initiatives, particularly in the Indo-Pacific and Europe, that include binding and enforceable digital disciplines and remove discriminatory barriers and promote economic inclusivity.

Working together, Congress, the administration, industry, labor, farmers, environmental groups, and other stakeholders can shape a digital policy that is both ambitious and inclusive.

The digital economy, as you so aptly pointed out in your opening remarks, touches all aspects of our lives, from texting friends, to working or shopping online, using digital technology, services and software on the factory floor; from design and production, to aftersales and service of autos, tractors, planes, consumer goods, and other products, to doctors conducting heart surgery with the aid of digital services and technology.

In 2021, the digital economy generated $3.7 trillion in growth output, over 10 percent of total U.S. GDP, and supported 8 million U.S. jobs. Many U.S. jobs, both blue and white collar, are now requiring digital skills. And it is critical that workers get the digital training they need to take advantage of those job opportunities.

Digital trade was and is a key source of resilience during the pandemic. From 2019 to 2021, digitally traded services exports in-

creased by $74 billion, while in a number of service sectors exports actually declined.

Senator CARPER. Repeat those numbers again.

Ms. BLISS. So, from 2019 to 2021, digitally traded services exports increased by $74 billion. And it is notable because, I think as we know, services exports in a number of sectors actually declined during that period. And, Mr. Chairman, in Delaware in 2021, services exports exceeded their 2019 level on the strength of digitally tradable exports, including financial and insurance services.

One-third of small businesses state that they would not have survived the pandemic without access to digital tools. Cloud services allowed manufacturers to continue their operations. The healthcare industry was able to expand its reach through telemedicine. Now Optics, a small business in Indiana, now provides virtual eye exams to patients across the U.S.

The digital economy also enables proliferation of small business. Estate Auctions, Inc., a Delaware-based small business with 14 employees, exported products to 62 countries using a digital eBay platform. Olaris, a woman-owned life sciences lab in Boston used AI to develop a noninvasive kidney transplant test. Marketing for Greatness, a Texas-based email sole-proprietor digital marketer led the international expansion of a Fortune 500 company. And Cloud to Street in New York, a woman-based, woman-owned small business uses digital tools to analyze flood risk and climate-vulnerable communities internationally.

Digital services allow small businesses in every single State to engage in global trade at a large scale. Good digital trade policy promotes American values like democracy and freedom, as was reflected in your remarks and Senator Cornyn's opening remarks. China and other authoritarian regimes are imposing their own digital rules of the road, which are at odds with these values and present national security concerns.

Like-minded trade partners should be standing shoulder to shoulder to defend democratic values through a rules-based trade system that adheres to longstanding norms of nondiscrimination and openness.

And we commend you, Mr. Carper, and Senator Young for your leadership in the resolution you introduced encouraging cooperation and coordination with allies, and also lifting digital trade barriers. We think that was incredibly useful.

We must address discriminatory services and digital trade barriers through strong digital disciplines that include AI principles, good regulatory practices for digitally enabled services standards, SME digital capacity building, and worker digital upscaling.

My written testimony lists CSI-specific recommendations, and IPEF seems to provide the most immediate opportunity to create these binding and enforceable rules. And it may also be a building block toward rejoining CPTPP. And we share the concerns and views that both you and Senator Cornyn expressed in that regard.

Congress has an important role to play in shaping these disciplines, and CSI supports a bipartisan extension of Trade Promotion Authority.

I thank you for this opportunity, and I look forward to answering your questions.

[The prepared statement of Ms. Bliss appears in the appendix.]

Senator CARPER. Madam President, thank you for those words.

Now, turning to our next witness, sitting on your left, is David Feith. David is the senior fellow of the Indo-Pacific Security Program at the Center for a New American Security. Do I have that right? Good. Center for a New American Security is a bipartisan think tank that focuses on developing strong and smart national security and defense policies.

Prior to his time at the Center for a New American Security, Mr. Feith served as the U.S. Deputy Assistant Secretary of State for East Asia and for Pacific Affairs. I am sure there is a lot more that I could say about you, but we are going to go on to give you the opportunity to talk.

With that, you have the floor. Welcome. We are glad to see you. I am looking forward to hearing your testimony.

STATEMENT OF DAVID FEITH, ADJUNCT SENIOR FELLOW, INDO-PACIFIC SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY, WASHINGTON, DC

Mr. FEITH. Thank you, Mr. Chairman. Thank you for your invitation and that of the ranking member, and I thank the whole subcommittee for this opportunity.

My written statement addresses digital trade and China, and in particular, the national security problem of China's open access to American data. It explains that America should not only work overseas to expand digital trade with our friends, but also move urgently at home to curb massive unregulated flows of sensitive data to China.

Now I would like to stress immediate action possible in three areas. First, to ban TikTok. Second, to begin controlling exports of Americans' biodata. And third, to implement a process endorsed by both the previous and current administrations, but not yet in use to limit U.S. data flows to China.

Now, in our unfortunately polarized politics, it is a sign of health that there is strong bipartisan support for countering China's threats. A major one is China's approach to digital trade, which is a key element of China's national security strategy.

China's leader Xi Jinping says that data in the 21st century is like oil in the 20th century—the critical input for economic strength and national power. About a decade ago, Xi declared: "The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will have the upper hand."

Under Xi, the Chinese Communist Party has made a strategic priority of exploiting data both inside China and around the world. This includes personal health records, genetic sequences, and online browsing habits. It includes corporate trade secrets, supply chain records, and financial accounts. And it includes the photos, voice recordings, and mapping imagery pulsing through the world's smartphones—as the chairman noted—and drones and smart cars.

Data control is also critical for China's global influence and censorship operations; hence, Beijing's aggressive regulation of Chi-

nese apps such as TikTok. Through that app, Beijing harvests massive amounts of American data and transmits favored messages, gives censorship guidance, and can influence young Americans in ways that are without precedent for a foreign power in history.

All this is the stuff of digital trade. Yet there are effectively no rules governing any of it—not international trade rules, and not domestic regulations.

My written testimony cites some additional issues, such as the importance of Japan's admirable initiative in this field known as Data Free Flow with Trust. But in the time available, for immediate focus I will note that U.S. policy can prioritize at least three areas.

First, TikTok, and the TikToks to come. The Biden administration is reviewing national security dangers posed by TikTok. Republicans Marco Rubio and Mike Gallagher have urged legislation to enable a ban. Democratic Senator Mark Warner, a member of this committee, recently endorsed a TikTok ban in principle, calling the platform an enormous threat.

The TikTok issue is a test of our seriousness about data privacy, counterintelligence, election integrity, and democratic sovereignty. No hostile foreign power is entitled to control a leading U.S. media platform, and keeping hostile foreign powers from wielding such influence is a safeguard of our free speech. But TikTok is also a test for the data threats still looming on the horizon, like China's ambition to export metaverse companies to the U.S. market, as it has for social media.

A second immediate matter: biodata. Clearly, Americans should protect their health and genomic and medical data to safeguard both privacy and national security. Yet our laws and policies do not do this. President Biden has announced measures to promote domestic biotech, but we still have effectively no protections regarding exports of biodata.

While we struggle with this, Chinese companies such as WuXi AppTec and BGI are expanding operations in the United States. These companies answer to Beijing's party-state and military. China's access to U.S. health data, and especially DNA, threatens harms with multigenerational consequences.

Third and finally, the importance of the new regulatory mechanism known as ICTS. This may be the best tool Washington has for all these issues. It could address a range of problems, including, for starters, data centers.

But the Commerce Department has not yet taken enforcement action against Chinese firms that may be improperly accessing so-called "large data repositories," despite a 2021 executive order threatening action. In drones too, the Pentagon has tied Chinese drone giant DJI to China's military. Yet DJI still dominates the U.S. commercial market. There are other Chinese players in the U.S. commercial market, such as Autel. Drones have not been the subject of any known ICTS enforcement action or even investigation.

Then there are autonomous vehicles and digital mapping. Many leading U.S. companies in these fields rely on Chinese financing and engineering, yet they can freely export sensitive data about U.S. roads, maps, and critical infrastructure.

ICTS, led by the Commerce Department, has a mandate to address all these issues—data centers, drones, autonomous vehicles, and more—but has not yet taken action. This issue would seem to warrant attention from the White House and the Congress.

As we have said, digital trade and China's threats to U.S. security are overlapping fields of bipartisan concern. So, it is a privilege to appear today. The stakes are very high, and I thank you for holding the hearing.

[The prepared statement of Mr. Feith appears in the appendix.]

Senator CARPER. And we thank you. Thanks for joining us. It is very nice to meet you, and welcome.

Our third witness—we have four; three witnesses in person. Our third witness in person is Dr. Joshua Meltzer, who is a senior fellow at the Brookings Institution, where his research focuses on international economic relations and the intersection of technology and trade policy. Is that right? Good. Dr. Meltzer also leads the Digital Economy and Trade Project and co-leads the Forum for Cooperation on Artificial Intelligence.

Prior to Brookings, he spent 8 years at the Australian Department of Foreign Affairs and Trade as a trade negotiator and as a diplomat at the Australian Embassy in Washington, DC.

Are you a native of Australia? Oh, good. Well, Dr. Meltzer, we are delighted that you are here. The floor is all yours. Thank you, and welcome.

STATEMENT OF JOSHUA P. MELTZER, S.J.D., SENIOR FELLOW, GLOBAL ECONOMY AND DEVELOPMENT, BROOKINGS INSTITUTION, WASHINGTON, DC

Dr. MELTZER. Chairman Carper, Ranking Member Cornyn, and members of the subcommittee, I thank you for the opportunity to testify today. I am a senior fellow at the Brookings Institution, where I work on digital trade issues, as well as on emerging technology such as artificial intelligence.

Today my testimony will address the opportunities of e-commerce and digital services trade for the U.S., with a focus on small and medium-sized enterprises. I will also discuss evolving global AI regulation and how trade policy can support digital trade consistent with U.S. values and strategic objectives.

As you noted, Senator, there is no globally agreed definition of "digital trade." However, it is a term increasingly used to describe an ecosystem that is more expansive than e-commerce, and includes cross-border data flows and how data and digital technology such as cloud computing and AI enable trade.

Trade agreements now have digital trade chapters instead of e-commerce chapters that include new commitments, such as not to prohibit cross-border data flows and required data localization as a condition for doing business, subject to GATTs Article XIV style exceptions.

Digital trade chapters aim to encourage regulation that builds trust in cross-border data flows. Digital trade commitments can deliver significant economic gains for the U.S. The 2019 U.S. ITC assessment of the economic impacts of USMCA found that the digital trade chapter is a key driver of the economic gains for the U.S. These rules were found to have significant positive impacts on in-

dustries that rely on cross-border data flows, including for firms in the services' economy, manufacturing, and agricultural industries.

One aspect of digital trade is e-commerce, which represents a real opportunity for small businesses to export and reach customers globally. A key development has been platforms such as eBay, Amazon, Etsy, Mercado Libre in South America, and Lazada in Asia, to mention a few.

These platforms solve many of the barriers that have previously prevented small businesses from exporting by providing integrated payment solutions, trust mechanisms, cheap and effective dispute settlement, and links to express delivery services.

The opportunity for small businesses to engage in digital trade has been enabled by trade policy. The WTO Trade Facilitation Agreement reduces the costs of getting goods through Customs. USMCA raised the *de minimis* Customs duty levels in Canada and Mexico, which has led to increased e-commerce sales. Commitments on electronic signatures and electronic authentication provide important legal frameworks that allow for digital cross-border transactions, and commitments to not restrict data flows and to encourage interoperability among digital payment systems also enable e-commerce.

Services exported online are another growth opportunity for the U.S. The U.S. has been exporting more services than it imports for over 30 years, and services now comprise around 40 percent of total U.S. trade. But services are an even more significant share than that. This is because around 30 percent of U.S. goods exports comprise value-added services used in the production of goods, the net result being that over 60 percent of total U.S. exports comprise services. And a lot of these services can be exported online.

Recent OECD data shows that the U.S. is the world's largest exporter of digitally deliverable commercial services, over three times larger than its nearest competitor, Germany, and 2.2 times larger than the UK.

While digital trade is an opportunity for U.S. businesses, the OECD Digital Services Trade Restrictiveness Index shows high levels of digital trade restrictions globally. This includes in countries such as India and Indonesia that are participating in the Indo-Pacific Economic Framework negotiations, and the digital trade restrictions in these countries pale in comparison to China, which is one of the world's most restrictive digital trade regimes.

Digital trade also affects access to and the development of key digital technologies such as AI. Recently, U.S. National Security Advisor Jake Sullivan identified three families of technologies including computer-related technology that includes AI, which he described as "force multiplied" throughout the tech ecosystem, where U.S. leadership is needed from a national security imperative.

While the U.S. is a world leader in AI, many countries are moving to regulate AI and expand AI R&D cooperation. China, second only to the U.S. in terms of AI capacity, has begun to roll out its own AI governance framework, which includes regulations on the development and deployment of AI algorithms, as well as increased control over Chinese technology firms leading in AI development. China is also exporting its model for AI regulation to other countries in the Indo-Pacific and globally.

Some countries are now using trade agreements to support AI specifically, but the U.S. has yet to do so. The U.S. certainly is the largest and most innovative digital economy that creates opportunity for digital trade for both small and large businesses. The U.S. has led development of digital trade rules in the USMCA and CPTPP, but renewed U.S. leadership is needed to develop rules that govern digital trade more broadly.

Yet, while the U.S. decides what to do, the world is not standing still. China is leading the development of rules in digital trade in RCEP and is seeking to join the CPTPP, where it will be able to influence the next generation of digital trade commitments.

The forthcoming IPEF negotiations are the next opportunity for the U.S. to reengage in the development of digital trade rules that support economic opportunities for U.S. firms and workers, and to shape the global context.

Thank you.

[The prepared statement of Dr. Meltzer appears in the appendix.]

Senator CORNYN. We are in the process of voting, so Senator Carper stepped out. So I will introduce our final witness, Mr. Patrick Woodall, the policy and research director at the AFL–CIO Technology Institute. He also serves as a board member for the Trade Justice Education Fund, which is a nonprofit that sponsors public education programs designed to expand awareness about the worker rights, environmental and climate, and public health implications of U.S. trade policy. He has been a policy expert and researcher for 3 decades, advocating for economic and social justice.

Mr. Woodall, you have the floor.

STATEMENT OF PATRICK WOODALL, POLICY AND RESEARCH DIRECTOR, AFL–CIO TECHNOLOGY INSTITUTE, WASHINGTON, DC

Mr. WOODALL. Thank you very much, Ranking Member Cornyn, and Chairman Carper, and members of the committee. It is a great opportunity to testify today. I am here on behalf of the AFL–CIO Technology Institute, the AFL–CIO, and the more than 12 million union members working in every State and every sector of the economy.

The labor movement is deeply interested in international trade policy. Trade deals have cost millions of manufacturing and service-sector jobs, upending the economic security of working families, and worsening America's economic and racial inequality. But we are focused on digital trade as well. The digital discussion frequently sounds like it has no grounding in the physical world, which Ranking Member Cornyn referred to. It is Internet-enabled commerce, and big data, and cloud computing. It is all of those things, but it affects real workers in the physical world, because cross-border digital commerce has offshored tens of thousands of U.S. call center and back-office jobs, and this low-road offshoring has fueled a digital underclass of gig workers in the developing world that power artificial intelligence systems. These ghost workers tag images and code information for low pay, including in India and the Philippines, which have notoriously poor working conditions and weak labor laws. And digital trade powers automated decision-making and algorithmic management software that in-

creasingly hires, controls, evaluates, monitors, and even fires workers in the United States.

These technologies can shortchange workers' earnings, expose workers to unsafe 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 compromise everyone's privacy. The algorithms, the power of social media, have pushed online hate, spread political disinformation, and harmed the mental health of young people.

But the existing trade model makes it harder to safeguard workers, consumers, and society from the known and emerging downsides of the digital economy.

First, the current digital trade deals grant broad, unfettered powers to companies to shift data and deploy software worldwide. These authorities over data and software are more expansive than for trade rules on physical goods.

Second, the digital trade rules rigidly limit or forbid government oversight of the technology sector, as well as its data and its software products. The technology industry appears to view any oversight, including efforts to safeguard digital privacy, as illegitimate trade barriers. The digital provisions almost read like high-tech commandments: thou shalt not limit cross-border data flows; thou shalt now require any data to be maintained domestically; thou shalt not look at the source codes that power software that affects workers and consumers. Since the 1990s, trade agreements have constrained domestic governance to curb so-called non-tariff trade barriers. Longstanding regulatory approaches have been subjected to trade tests to determine if they are permissible rules or illegal trade barriers.

At the WTO, fewer than 5 percent of challenged regulations have been upheld in trade disputes. The stringent regulatory restrictions in digital trade are fundamentally different because we are just starting to grapple with meaningful oversight of these technologies. It will be easier to challenge efforts to rein in the downside to these technologies as illegal trade barriers because of our limited legal and regulatory foundation.

Bipartisan efforts to protect personal data or address anti-competitive platform practices could run afoul of existing digital trade language. So the combination of unilateral corporate powers and narrow regulatory constraints in digital trade can lock in a largely unregulated technology landscape.

It is time for sort of a strategic reset to create a worker-centered digital trade policy. This is not a binary choice between China's Great Firewall and a totally unregulated technology sector. We must be able to protect personal information in critical sectors by establishing restrictions on vulnerable cross-border data flows.

Digital trade deals should encourage rather than deter government efforts to protect personal data inside and outside the workplace. Safeguarding critical infrastructure and personal data not only protects the security of the economy and people, but it also helps keep good jobs here in the U.S.

We must be able to meaningfully oversee source codes and algorithms to robustly enforce current labor and employment laws, and enact new laws to address emerging issues like electronic workplace surveillance and digital privacy.

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

Thank you for the opportunity to testify, and I am happy to answer any questions.

[The prepared statement of Mr. Woodall appears in the appendix.]

Senator CORNYN. Thank you, Mr. Woodall.

Senator Carper, the chairman, is not back, so I will proceed with some questions, and I am sure I will turn it over to him when he returns.

Dr. Meltzer, I am looking at your testimony here. I was not here for the beginning of the answers to Senator Carper's questions, but I will just read this.

You say, "There's no globally agreed definition of digital trade. However, it is a term increasingly used to describe an ecosystem that is more expansive than e-commerce, which is focused on trade in goods and services purchased online. Digital trade includes the important role of cross-border data flows and how data and digital technologies such as cloud computing and artificial intelligence can enable trade."

Did I read that correctly?

Dr. MELTZER. Yes, Senator.

Senator CORNYN. And let me just ask our other witnesses. Ms. Bliss, do you agree with that definition? Or do you have any differences?

Ms. BLISS. No, I do not have differences. And I think that Dr. Meltzer has adequately described it. And in my written testimony, we tried to elaborate that, in our digital economy certainly, are what are referred to as the pipes—the infrastructure, the fiber-optic cables, the technology that enables the Internet—and then the platforms, technologies, software, and services that build onto that to enable the functioning of the digital economy itself.

And then of course all the various apps that are being developed and the emerging technologies in that space. And then, I guess at the core you could say that it is about electronic transmission of data across the Internet and the content that is included there. But I would be in agreement.

Senator CORNYN. Mr. Feith, I know you focused on national security aspects of this issue. Obviously the Internet has proved to be a boon to businesses and individuals to share information, and of course we are a free society where people are free to communicate. But our adversaries, particularly the People's Republic of China and the Russian Federation, use information warfare essentially to steal our data, and then to do everything from engaging in disinformation or active-measures campaigns like they did in 2016 during the presidential election.

Talk to me about the benefits of us entering into some digital trade agreement with our democratic allies, and how that plays

into this sort of split personality when it comes to digital information in a free society versus autocratic societies.

Mr. FEITH. Thanks, Senator. I think the split personality point is well put. And I think that some of your definitional questions, and the answers we have heard, also highlight a really valuable and important quality of this whole discussion, which is that some of what makes this difficult and dangerous as an issue—when it comes to the role of hostile adversary countries in digital trade and in our domestic digital economy—is that the nature of so much of digital trade is unlike the nature of traditional trade that passed in physical goods by truck and ship and horseback over the years, where fundamentally there was a structure among nations where the trade was controlled at borders and arranged between countries according to agreements.

The Internet was born and then established with none of that. There was no need to go open any other countries. We all allowed the Internet to emerge all over the world. And as we have said, there were enormous benefits to this in matters of prosperity and quality of life and all the rest.

And yet it caused also the national security challenges that we face today. In a way completely without analogy to the physical trade in goods, we have adversary country state actors and state-backed actors operating in our telecommunications networks, across our digital economy—meaning in our pipes, in the platforms of the delivery of these digital goods and services, and in our politics through the use of platforms like TikTok and other social media platforms—where not only can data be harvested, but the export of the censorship and propaganda objectives of the Chinese Communist Party, for example, can be done at scale and in a fashion that was simply impossible in the pre-digital age. And we do not have mechanisms in our international trade rules, and we really do not have mechanisms even in our domestic regulation, for dealing with this.

We have the Committee on Foreign Investment for handling inbound foreign investment. We have export controls for licensing and restricting the traditional export overseas of goods and services and some technologies. We have Federal procurement restrictions that restrict what Federal departments and agencies and their contractors can purchase.

But our Federal regulatory structures have traditionally been just silent on an enormous range of domestic digital commerce that has international digital trade implications. And that has to do with what people put on their phones, what companies do when it comes to their drones or their surveillance cameras. It has to do with the handling and sharing overseas of our most absolutely sensitive data, such as our genomic DNA information.

These things have been effectively untouched by the traditional tools that we know for national security—you know, restrictions and approaches to matters of commerce. And that is partly why we have such a challenge here.

It is also partly why this new ICTS regime represents such a potentially valuable and important new element of the national security regulatory mix, because we now have had on paper the creation of this institution. It is like CFIUS, but it is for cross-border

data flows. And instead of being led by the Treasury Department, it is led by the Commerce Department.

It was put out initially in the waning period of the last administration, endorsed in the first months of the current administration, but it exists only on paper. It has never actually taken action, not against data centers, not against drones, not against autonomous vehicles and digital mapping, and not against anything relating to the biodata-particular priority. And it would appear that the case for that is really just very strong and rather overdue.

Senator CORNYN. Thank you.

Senator CARPER. I thank my colleague. I think, since I was off voting, we have been joined by our chairman of the full committee, Senator Wyden. Welcome. Thank you for joining us. Catherine Cortez Masto, Catherine, it is wonderful to see you. Thank you so much for joining us. And also, we are joined by a new member of our team, Senator Grassley, a new member of the Senate. [Laughter.] He has been here actually as long—how many years have you served in the Senate now?

Senator GRASSLEY. Forty-two.

Senator CARPER. Forty-two, but who is counting? That is great. You have seen a lot——

Senator GRASSLEY. It is just a number.

Senator CARPER. It is just a number. That is great. Well, congratulations to both of you on your re-elections, and I am delighted you were able to join us today.

My first question is pretty easy. Several of our witnesses have used the term "ICTS regime." People watching us on television probably have no idea what you are talking about. I am not very good at acronyms.

How would you, Mr. Feith—how would you explain that to your grandmother?

Mr. FEITH. The unpronounceable acronym happens to stand for Information and Communications Technology and Services, which is not how I would begin the explanation for my grandmother, though.

Senator CARPER. Is your grandmother still alive? Is she still alive? She might be watching us.

Mr. FEITH. No, unfortunately not, but we have a daughter who is named for her, so that is an alternative.

Senator CARPER. That is good. The next best thing.

Mr. FEITH. This is meant to be a structure inside the U.S. Government that pulls together expertise from all the relevant parts of the executive branch—national security departments and agencies, commercial and economic departments and agencies—and the intelligence community, in order to assess the national security implications and risks of all of the enormous flows of data that could go cross-border, especially between the United States and the so-called foreign adversary countries, beginning with China and Russia.

Senator CARPER. All right. I think your grandmother would probably say, "That's my grandson. I am so proud of him." All right; thanks for doing that.

I have a question, really for all of our witnesses. I think we will lead off with Ms. Bliss, by asking you to respond to it initially.

As the leaders of this subcommittee, Senator Cornyn and I have long advocated for engagement with our allies in the Asia-Pacific region—you mentioned this—after the previous administration abandoned multilateral cooperation.

Now, as the Biden administration works to reclaim a seat at the table with our Indo-Pacific Economic Framework, digital trade presents a clear opportunity for U.S. leadership in this critical region.

We know that both our allies and our adversaries in the region are racing to write the rules of the road on digital trade, and our allies have been clear that they welcome our partnership on the digital trade in order to advance our shared values.

Here is my question for each of you: what specific digital trade policies should the United States advocate for in the Indo-Pacific Economic Framework? I will say that again. What specific digital trade policies should the United States advocate for in the Indo-Pacific Economic Framework in order to advance our economic, security, and geopolitical interests? Ms. Bliss, would you be our lead-off hitter there? And then Mr. Feith, and then we will go down the line.

Ms. BLISS. Thank you, Mr. Chairman. And we did supply to the committee, as an annex, our specific recommendations with regard to IPEF—and more generally in terms of what we believe should be included in the digital chapter. But let me highlight some areas.

That is, we think about the provisions that were included in the bipartisan USMCA digital chapter, and then building on that, the U.S. and Japan also looking to some of the innovations that have been made by our trade partners in the region. Australia, Singapore, and others provide important new elements that can be included. At its core—and I think you have listed this in your resolution—we need to certainly address cross-border data flows. And I would point out that it is not the case that there is an absolute allowance of cross-border data flows in all circumstances. There is provision for deterrence from that, where there are legitimate public policy objectives. And that is certainly something that we would want to see continued.

Too, data localization is pernicious and increasing, and has wide implications, particularly in respect to challenges posed by China. And I think it also relates to the data issues that have been raised here today.

And I also believe that the source code provisions, which again are not absolute—it is not an absolute prohibition on mandatory transfer of source code. There are exceptions to that for law enforcement for not just judicial processes but also regulators, inspections, and other circumstances. So I just want to correct the record that that source code provision is not absolute.

I also want to emphasize the importance of a permanent moratorium on e-commerce duties, and also new provisions that we have suggested, including things like AI best practices principles, which we think can address some of the issues that have been raised, particularly in Mr. Woodall's testimony, with regard to concerns about potential abuses of AI in the workplace.

We also think it is very important that there be a commitment to worker upscaling in the digital area. We also think that inclusion of tools for small businesses is incredibly important. And cer-

tainly, greater inclusivity is very important. And I also should mention addressing the pernicious problem of censorship that I think is another area that should be addressed.

Senator CARPER. Good. Thank you for that comprehensive response. My time has expired, and we will come back later in the hearing, and we will have an opportunity to invite our other witnesses to respond to the same question.

The next person to recognize for questions is Senator Grassley, and then Senator Cortez Masto. So, Senator Grassley, you are up, followed by Senator Cortez Masto.

Senator GRASSLEY. Thank you.

I am going to start with Mr. Feith. We are all concerned about national security and protecting the data flow, and we are concerned about consumers, making sure that their technology is protected. And obviously we think mostly about the Chinese Communist Party and China generally in this regard.

So my first question is, you have stated the need to ban TikTok and digital platforms that are similar. Could you explain why this is necessary?

Mr. FEITH. Thank you, Senator. The threats posed by TikTok—and, as your question suggests, by other platforms, and there are many that are subject to the same Chinese Communist Party influence and control and subversion—involve both data that would flow out of the United States to China, and the data in a sense that flows from Beijing and its political edicts into our digital economy.

In that first category, you have the sort of relatively more commonly recognized data privacy concern, which is that TikTok is on the phone of 100 million or more Americans. TikTok in public statements and in congressional testimony has given a whole range of often contradictory and questionable answers about how they can possibly keep that data that is on American phones and in the TikTok app from the Chinese Communist Party, given the nature of Chinese law.

It would appear completely impossible, because the laws—including the National Intelligence Law of China, the Cybersecurity Law of China, more recently the Data Security Law of China, and others—make absolute the demands of the Chinese Communist Party to unchecked access to data that touches Chinese platforms like TikTok. And so the risk of the harvesting of that data from all the American users is enormous.

There is also, though, the somewhat less widely recognized set of risks involving the effect of the export of censorship from the Chinese Communist Party to the American public when so much of the American public relies on this platform for news—news about the world, news about our elections, and possibly the news in future circumstances that might involve Taiwan, might involve different actions in which the U.S. and China are adverse. And the ability of TikTok to be a platform for the mass manipulation and even mobilization of American users—dictated by and consistent with the hostile political aims of the Chinese Communist Party to which TikTok has to answer by virtue of Chinese law—is a very grave threat.

Senator GRASSLEY. What other countries are there that we have to worry about getting into Americans' data? Are there other countries that pose the same problem as China or near that?

Mr. FEITH. There are certainly other countries that pose similar problems. There would not appear to be any other country that poses the problems at the magnitude and severity of China.

I would note, for example, that the Biden administration put out in June of 2021 an Executive Order on Protecting Americans' Data From Foreign Adversaries. That "foreign adversaries" category, I believe, pursuant to some regs from the last administration, affects six countries: China, Russia, Iran, North Korea, Cuba, and perhaps Venezuela. I would want to check that, but I believe that is the set of foreign adversary countries.

Several of the questions we have discussed have mentioned China and Russia together. Certainly those two would appear to stand out on the list of six, but even still, there are not Russian platforms with a presence in the United States anything like the Chinese platforms. And the Chinese platform concern, and the Chinese digital economy and digital trade concern, is hardly limited to TikTok. You know, TikTok's parent company, ByteDance, has a new virtual reality company, a subsidiary called PICO, which has ambitions for the U.S. metaverse market to compete here domestically against Facebook and Apple and all the others.

There are a wide range of social media payments and other platforms that come from China. They are widely used because they are good apps. But they also pose these enormous challenges that are often difficult for consumers to keep track of. They are often really only a threat in the aggregate, when you talk about the aggregate of all of this data and what a foreign adversary government can do with it.

But that is why it seems to pose these national security concerns that warrant attention here.

Senator GRASSLEY. My time is up.

Senator CARPER. Senator Cortez Masto, you are up. Thanks for joining us today.

Senator CORTEZ MASTO. Thank you. Thank you for this great subcommittee hearing, and I appreciate everybody who is participating today.

Let me, Mr. Feith—is it Faith? Feith?

Mr. FEITH. Feith.

Senator CORTEZ MASTO. Mr. Feith. Let me start with you, because you talked about data harvesting. How long would you say data harvesting has been going on? How many years?

Mr. FEITH. Roughly as long as we have had data.

Senator CORTEZ MASTO. And so, do you think it is too late to start putting in regulatory regimes to protect, let's just say, an individual's PII?

Mr. FEITH. No. Some harm is irreversible, but a lot of harm is still ahead of us.

Senator CORTEZ MASTO. And when you are talking about "harm," identify that harm. What does it look like?

Mr. FEITH. I think we can talk about it in various ways. There is the exposure of private information that is of potential intelligence value.

Senator CORTEZ MASTO. So, national security. That is something we always would address. But let's talk about individuals, because one of the things you talked about, which I am very concerned about—but I am also concerned that it might be too late—is protections for biodata. We definitely need to do something, as you have said. But is it too late? I mean, that information is already out there for many, and you cannot pull it back. So how would we address that?

Mr. FEITH. I think the observation that there have been transfers here that are harmful and that that harm cannot be remedied, I would agree with completely, for transfers that have already happened. And yet I would also be inclined to say that there are uses of biodata that are currently devised but are imperfect and will still need to be fed by enormous amounts of data that companies and governments will seek to ingest over time. But some will seek to do so in ways that are generally consistent with democratic values and the rule of law, and some will do so in the way that the Chinese Community Party functions.

Preventing the future ingestion of that sort of data over time for these uses of biodata already devised would seem to be a major interest of ours. There are also, one would think, infinite uses of biodata not yet devised that will come about in the future——

Senator CORTEZ MASTO. That we do not even contemplate. With new technology and everything that is out there, it will be there. I agree with you. I agree with you. And I think this is part of our challenge: trying to figure out what this regulatory regime looks like, and what data—what we are trying to protect.

Mr. FEITH. And if I could just note, in addition to the ICTS process, which is an administrative instrument that is out there and that has an important mandate to go implement, I would note—Senator Wyden was here and has left, I see, but he introduced a bill that has several Republican cosponsors—and I think also Senator Whitehouse might be on the bill as well—back in June to create a new export control category for bulk American data. And so this would essentially take the export control system that we have long had at the Commerce Department, led by its Bureau of Industry and Security, and create a new element of it to focus on the bulk transfer of American personal data, in principle, to try to combat all of these sorts of risks.

There are enormous complications for how exactly this would be done. I would just observe that it is notable—and I think unfortunate—that that bill pointing at a really important national security China-related concern that we have, is not the subject of more debate and consideration, including, for example, in the major legislative process that you all completed this summer with the CHIPS Act. And so it would seem another opportunity in the new Congress, presumably, to look at that effort and other ways of getting at that same very important problem.

Senator CORTEZ MASTO. I agree. Thank you. And so, what I am hearing from you today is, the ICTS committee concept on the white paper is a good start, it is where we should be starting here?

Mr. FEITH. Yes, ma'am.

Senator CORTEZ MASTO. Is there any state—I am curious—is there any state that you guys are aware of that has put in protections that we should be looking at, that is a good model?

Mr. FEITH. I will happily defer to colleagues as well. I would just note that the short answer would appear to be "no." The Europeans, through their GDPR, have a much more aggressive and mature and advanced data privacy framework. But they have been mostly directing it against the United States and our big tech players and questions about the Privacy Shield, and what the U.S. Government might do with European personal data that gets sent across the Atlantic.

The European approach to data, for all of its vigor, has been rather uninterested in the fact that the data protections for Europeans in China are nil. And the Chinese platforms, of course, operate in Europe as well.

Senator CORTEZ MASTO. Thank you.

Thank you, Mr. Chairman.

Senator CARPER. Senator Cortez Masto, I thank you.

Senator Casey was here, and he had to leave. He may be back, and when he comes back, I will recognize him. Senator Wyden was here and had to leave for a while. I think he will be back, and I will recognize him.

But meanwhile, live and in person, Senator Young. Welcome. He is somebody who shares my passion for these issues, and we appreciate very much his leadership and allowing me to be his wing man on some of them. Thank you.

Senator YOUNG. Thank you, Mr. Chairman.

I want to thank our panelists for speaking to this important issue of digital trade. I see incredible opportunities and some risk as we try and plot our way forward. The risk, I think, emerges because there is a sense of urgency—at least I feel it—for the United States to work with partners and allies to kind of further refine our rules in this area. And as it relates to this area, as with so many other international policies, we need to come up with rules that are somewhat flexible, that are consistent across international boundaries.

So there are a lot of commonalities between the work that I think is going to be required here and what we do in other areas. We also need to make sure that we are effective. We have to make sure our digital trade rules can prevent the bad actors from purloining our data and preventing us from growing to the extent we otherwise would, and landing market shares, since the United States leads in some of these areas, from digital platform to digital services, and so forth.

And I think we can do a real service to many of our allied countries across the Indo-Pacific in particular, and others. There has been much conversation about that here today.

The administration, I think appropriately, has recognized the importance of the Indo-Pacific. The digital trade pillar within IPEF recognized the importance of this issue. But I feel like a more targeted approach is necessary. And I know colleagues on both sides of the aisle agree with me with respect to that. The chairman and I have just introduced a resolution, in fact, indicating our belief in

the importance of this area, and we hope that continues to gain more support.

My first question would be of Ms. Bliss. We have some recent experience in this area of digital trade rulemaking with USMCA. I am just looking at a punch list of things that are included there. USMCA prohibits Custom duties on digital products. There is a commitment to nondiscrimination, localization requirements, no forced disclosure of source codes and algorithms. It requires parties to establish civil and criminal procedures and penalties for trade secret theft. And it recognizes risk-based approaches and the need for strength and cooperation between governments on cybersecurity. Those are among the things that are called for in the USMCA.

How is this different, as we look at the Indo-Pacific context? Just very briefly, what differences will be required to cater to the Indo-Pacific countries?

Ms. BLISS. Well, first of all, I want to commend you, as I did Senator Carper, for your leadership in introducing your resolution on digital trade, and working with allies, and listing barriers. That has been very effective and important.

But to your point, I think that because we are not in an FTA negotiation, and we are looking at a different kind of initiative that does not directly offer market access, one of the challenges is going to be how we convince some of our countries that may not be like-minded but that are participating in the trade pillar on the digital piece to come on board in the high-level standards.

So one of the differences I would point to is, I think it is going to be very important that we do build in incentives like capacity building, hopefully encouraging countries like Indonesia, Thailand, Vietnam, Malaysia, to create environments that will attract foreign investment, which we know they desperately want.

The other thing I would point out is that I think another difference is that we think it is really important to include some new provisions that go beyond what was done in USMCA and U.S.-Japan. And I have outlined that to the committee previously, but just, for example, I think we absolutely need to include principles on AI. I think that is very important.

I think we also need to include something on digital worker upscaling. I think that is important for U.S. workers as well, as it is for IPEF countries.

I think we need to include something on SME digital tools, and something on greater inclusivity, just to name a few. And I also want to highlight for the discussion, particularly some of the remarks that Mr. Feith had made, that cybersecurity, I think, is a very important area that we need to build on as well.

Senator YOUNG. Thank you for that. There is just so much here. It is a very broad topic, and good subcommittee hearings typically are based on broad topics that give us an opportunity to move into a number of areas.

So one of the areas that I know my constituents are interested in is the national security implications of digital trade, and maybe not getting the rules right as we try and address certain challenges.

So I would like to ask Mr. Feith some questions in this area. Mr. Feith, specifically I am interested in the challenges some of my col-

leagues have brought up with China. China is one of the most digitally restrictive economies in the world, but it is also one of the largest consumer markets in the world.

And in your testimony, you covered many examples to show how the Chinese Communist Party is accumulating and exploiting data, and pushing policies that allow them to selfishly advance their own authoritarian interests.

So, Mr. Feith, I will just ask you an open-ended question here. What is at stake if we sit back and we let China dictate standards in digital trade? What is at stake if the United States fails to boldly solidify some international standards, especially as we look at the Asia-Pacific area?

Mr. FEITH. Well, thanks, Senator. As with many things China, taking seriously the words of the Chinese Communist Party leadership and of Xi Jinping can be instructive on this issue.

What he has said is at stake in the contest over data, and over which countries and political systems are best able to recognize the significance of data and exploit data—he has said it is the matter of the upper hand in future world power.

He has been saying this actually for quite a while. It was 10 years ago that he compared data in our century to oil in the last century as the most important component of economic and therefore national power.

Senator YOUNG. And do you agree with his assessment?

Mr. FEITH. Yes. Not because it is his, but because there is an insight there.

Senator YOUNG. In fact, I think each of us would be wise not to dismiss his assessment because it happens to come from a Chinese Communist leader, right?

Mr. FEITH. Yes, sir.

Senator YOUNG. Thank you, Mr. Feith.

Mr. Chairman, I yield back.

Senator CARPER. There was a great song I heard the other day, "You've Gotta Have Faith." There is no song that has ever said you've got to have Feith. Has anybody ever mispronounced your name, Mr. Feith?

Mr. FEITH. It has been done.

Senator CARPER. Even today. I like to say "Feith" as in "wife."

Senator YOUNG. It is an excellent mnemonic device.

Senator CARPER. We are rejoined by our committee chairman, Senator Wyden. Thank you so much for being here.

Senator WYDEN. Thank you, Senator Carper. The election is supposed to be over, but things are just as hectic as before.

I am going to ask you a question, if I might, Dr. Meltzer. Obviously businesses and workers and consumers understand that in our country, the Internet is free and open. And having come to the United States Senate when virtually nobody knew how to use a computer, that was something that I have been dedicated to, that proposition, ever since I had the honor of coming here.

So our Internet is free and open. Communist China builds its Great Firewall higher and higher year after year, shutting out our businesses and crushing dissent. We are obviously watching on our TV screens today the way the regime censors protests, pushes back against the COVID lockdown, and brutally cracks down on dissent.

My view is that we are watching, every night, a human rights disaster unfold, and it is spreading like wildfire with our trading partners in India, Vietnam, and Indonesia. All across the world, for example, surveillance is becoming the new normal, and technology is used to monitor worker communications and stamp out dissent and organizing.

So I thought, because of your expertise, Dr. Meltzer, it would be helpful to have you briefly outline several of the smartest reforms that could be made to our trade policy to put the United States in a position to push back as effectively as possible against the human rights crackdowns.

Dr. MELTZER. Thank you, Senator, for the question. And I certainly agree with your observation in terms of what is unfolding at the moment. It is a dynamic space. And there is clearly an important role, I think, for U.S. leadership on digital trade policy issues as a key component of building an ecosystem—I think particularly in the Asia-Pacific region—which reaffirms the norm of an open and free Internet.

In many respects, this is sort of the center of where this broad or strategic conflict, I think between the U.S.—and I should say the West, really—and China is going to play out on the ground. And we see this happening in versions of trade policy which China is advocating, compared to what would be a preferred, I think, U.S. approach.

And one need only look at, for instance, the RCEP, the Regional Comprehensive Economic Partnership, which on one level is not a bad agreement, but includes a lot of loopholes and exceptions for China's approach to the Internet and restrictions on data flows, and so forth. And we have a lot of important countries in the region that are now party to that agreement, which has become a baseline for them. And you know, it refers specifically to the ASEAN countries, which are obviously part of the RCEP agreement. They are negotiating a digital economy framework agreement, probably starting next year, and that will be their starting point. And moving them towards a view of digital trade which is more consistent with the view that the United States has of what would be an appropriate way forward, in terms of data regulation and free flow of data, I think is an important objective here.

And part of achieving that is going to be U.S. reengagement, I think, on digital trade policy in the region.

Senator WYDEN. My time is going to run out shortly.

You are a member of this committee in a hypothetical question. What kinds of changes to our trade policy would you advocate, to our digital trade policies, in order to allow our country to push back as effectively as possible on these human rights violations?

Dr. MELTZER. Well, I think that it would require starting with what we have got and then using the full weight of access to the U.S. market to incentivize the region to adopt an approach to data flows and data regulation——

Senator WYDEN. What would be an example of such an incentive?

Dr. MELTZER. Well, I honestly think, Senator, that the IPEF may get us part of the way there, but I think it would take a comprehensive sort of trade agreement that built in a set of digital

trade rules that build on USMCA. But I think we need a lot more. We have heard a lot on this panel about what that might comprise, so I will not repeat that, but I think that the rules which are combined with enforcement, plus the incentive of access to the U.S. market as kind of the key piece, that kind of incentivizes compliance with the rules that are kind of the comprehensive——

Senator WYDEN. We are very much interested in incentives here in the Senate Finance Committee. The reason we got a breakthrough with respect to clean energy policy is, we wrote a piece of legislation that said the more you reduce carbon emissions, the bigger your tax savings.

So, you had us at "hello" on the proposition that incentives are a good thing. So we will hold the record open, with Chair Carper's permission, and I would be very interested in a couple of examples of your ways to tie these incentives. And open markets are certainly one possibility. But if we are going to actually put them down in the policy, we are going to need to be able to lay this out in a straightforward way.

That is what we did with respect to clean energy. After 20 years of gridlock, we said, "Hey, we are going to make this pretty simple. It is going to be technology-neutral. It is going to be market-oriented. Everybody is going to have a chance to be part of a new system. But the incentive is, you get the tax savings if you do what the public needs so desperately, which is to reduce carbon emissions."

So, if you can give us something that resembles that as it relates to digital trade markets, we will give you a parade and a hot fudge sundae. Okay?

Dr. MELTZER. Well, that is a great incentive for me, Senator. And I will add, on the incentive front, that there is an infrastructure component here, which is really a development issue in a lot of the world. When we talk about digital trade issues for a lot of the world, getting access to the Internet, sufficient broadband, is very crucial. And I think there is a role here for the U.S. to take a more significant place in supporting the infrastructure build and the investment that is needed in the digital space as well, which would then support the apps and the content services after that.

Senator WYDEN. Well, thank you.

Senator CARPER. Mr. Chairman, thank you so much for coming back and not being here just once but twice. We very much appreciate that and the help of your staff in putting this hearing together.

We have been joined by Senator Warren. It is great to see you. Thank you for joining us.

Senator WARREN. Well, thank you very much.

Senator CARPER. Please proceed. You are recognized for 2 hours. [Laughter.]

Senator WARREN. Thank you, Chairman Carper. And thank you very much for holding this hearing.

So, giant corporations use bad trade deals to pad their profits and to chip away at protections for workers and for consumers. And now that the U.S. and other governments are trying to rein in big tech, their lobbyists and lawyers are trying to rig digital trade rules to undermine those new regulatory laws.

They wrote some of the digital rules in the new NAFTA agreement, and now they are trying to rig the Indo-Pacific Economic Framework negotiations as well.

So, take artificial intelligence, or AI. Companies increasingly rely on AI, even though AI, for example, can discriminate systematically, rejecting a job or loan for an applicant for having a Black-sounding name, or penalizing a worker for a disability, or misidentifying women of color in police footage.

This raises big concerns. And Congress and regulators are now taking a very close look at what is going on. But big tech wants to keep its code in a black box where nobody gets to look at it.

Mr. Woodall, you are the policy director at the AFL–CIO Technology Institute. You are an expert on digital trade. Under the source code secrecy rules that big tech is now pushing as part of its digital trade agenda, could Congress pass pending legislation requiring that companies submit their AI code to the government, or to third parties say, to assess it for potential bias?

Mr. WOODALL. Senator, obviously Congress could pass those laws to address the discriminatory impacts of AI in the workplace, but they could run afoul of the digital trade rules and be vulnerable to a challenge or a trade dispute. Obviously, the sort of reliance on this "necessary and legitimate" clause, as a justification would be, I think, a little thin reed to hide behind. The question is, legitimate to whom? Necessary to whom? And recognizing that, in the digital and technology world, our sort of regulatory landscape is very, very thin.

Most of the other trade areas that have been built were—really, the WTO went into effect decades after we had environmental protections and workplace safety rules. So this is a very different sort of environment, where the digital trade has a different impact on the ability to address the known downsides of technology on workers and people.

Senator WARREN. Okay, so that is a really powerful point. Now, you know, tech lobbyists like to say that source code secrecy is about protecting trade secrets from China. But they have written the trade rules to apply to everyone, including U.S. regulators. Now the tech lobbyists will say the language includes exceptions that ensure that regulators can still get access.

So what I want to do is just take another, closer look at the fine print on this. Regulators can look at source code or algorithms for, quote, "a specific investigation, inspection, examination, enforcement, action, or judicial proceeding."

Mr. Woodall, could regulators really use this exception? Is this going to solve the problem?

Mr. WOODALL. I think it is a real concern, Senator. And the reason—there are a couple of reasons.

One is that this sort of flags the VW problem, right, where EPA got a whistleblower to send the source codes to EPA that flagged that there was a problem with VW spoofing emissions tests. Now the question is whether there would be an ability to know to pursue these kinds of investigations. It is really a "chicken and egg" problem, right? You have to know enough to be able to pursue the investigation. And so this specificity language could make it hard

to really know whether to launch an investigation without being able to see under the hood.

And then the second sort of problem with respect to specificity language is, it pretty much precludes sector-wide, or practice-wide investigations that regulators frequently pursue to see how consumers are protected, or what is going on in the workplace. So I think the recognition that there is a legitimate role for government is good, but narrowing it into a specific case really is a concern for us.

Senator WARREN. Okay. So I get your point. So big tech wants to protect whatever is in the black box from AI, and they not only want it protected from China, they want to protect it from U.S. regulators.

But of course big tech companies only care about secrecy when it is their secrets that they want to protect. Meanwhile, they are fighting to protect their ability to collect, to store, and to sell your data anywhere else that they want in the world. And that is why the tech lobbyists behind the trade rules prohibit any limits on the international transfer of data.

So what if we wanted, here in the United States, to put limits on the transfer of sensitive data, say period tracking data, or location data for people who visited abortion clinics? Especially we want to put limits to countries with poor data protections.

Mr. Woodall, big tech says we should not worry, because countries can still pass laws to protect data, so long as they fit under standard trade agreement language called the "legitimate public policy exception." But how often have countries actually succeeded in using this language to defend their laws protecting consumers or workers or the environment?

Mr. WOODALL. It is quite infrequent. Less than 5 percent of the cases at the WTO where regulations were challenged as illegal trade barriers were upheld under the necessary and legitimate type tests. So it is very difficult to survive under these particular policy caveats. But as I said, I think it is going to be harder with digital because we have so little regulatory infrastructure and foundation upon which to defend the legitimacy and necessity of the regulations.

So as we are sort of—look, this is a world where we are just beginning to confront the concerns with this. And there are a bunch of laws that are being considered in Congress that would affect the digital privacy and monopolistic platform practices that could run afoul of these digital trade rules.

I would add, on the privacy issue, that language in the USMCA specifically says it must be necessary and proportionate to the risk, which is sort of an even higher threshold to defend future privacy rules.

So, all of this—look, there is a good reason to consider protecting privacy and protecting the data that is behind privacy for things that have been said on this panel already, on things like biometrics, on health data, on financial data. There are good reasons to exclude those kinds of personal data from the free flow of data and data localization, and there are good reasons to exclude things like critical infrastructure, as has also been said today.

So I think, thinking about exceptions to these data provisions is essential going forward.

Senator WARREN. Okay. So, thank you. It is a very powerful point you make. We are barely at a 5-percent success rate on trying to enforce the exception, so you are saying it could be even worse under the conditions if we go forward in the digital area here.

You know, it is not a surprise that big tech is trying to weaponize digital trade rules. They know that the U.S. Congress is now considering bipartisan legislation to try to rein in big tech. So this is a move to fight back.

And let's be blunt. Big tech has a lot of friends. I have raised concerns about the revolving door between big tech and the agencies like the Commerce Department that are leading our digital trade negotiations.

We cannot let big tech hijack current trade negotiations like the Indo-Pacific Economic Framework. Voters want Congress to strengthen their digital rights, and our trade agenda must reflect that approach.

Thank you very much, Mr. Chairman, and I appreciate your indulgence for the long questions and answers.

Senator CARPER. I know we were happy to welcome you and indulge you as much as you needed. That was great. Thanks for that exchange. Thank you for the enthusiasm you bring to these subjects too.

The Small Business Administration does a lot to promote the establishment of small businesses—to grow them—and they push something, I think it rolls around every Saturday, maybe right after Thanksgiving, and they call it "Small Business Saturday." And the idea is to try to encourage people across the country to patronize our small businesses. I think it is a good thing. I enjoy doing that. We try to help to nurture all those small businesses, and a lot of times they grow up to be really big businesses.

I have a question that relates to small businesses, and some small businesses understand every word you are saying; others do not. And just keep that in mind as you respond to this question.

But I think, Ms. Bliss, I am going to ask you; Dr. Meltzer, you can join us as well. But the same question, and maybe, Ms. Bliss, you could go first. The question is, digital connectivity has the power to unlock tremendous opportunities, not just for big businesses or middle-sized businesses, but for small businesses too, by connecting them with consumers across the globe.

Some of the small businesses I visited with my staff just in the last couple of weeks—we have actually seen that with our own eyes and heard it with our own ears. However, small businesses often need additional support in order to access foreign markets and to reap the benefits of our digital economy.

The question: what resources can help small businesses participate in the digital economy? And how can digital trade rules facilitate new export opportunities for small and middle-sized entrepreneurs?

Ms. Bliss, would you go first?

Ms. BLISS. Thank you, Mr. Chairman. And you will forgive me, but I——

Senator CARPER. I forgive you. You do not have to ask me to forgive you. [Laughter.]

Ms. BLISS. I will just divert for one moment, and then I will answer your question. And that is, that I think it is unfortunate that there is an enduring perception among some that the digital agenda is about big tech and driven by big tech. And I think my organization is an example of that.

Yes, we do have several large tech companies, but they are only about 10 percent of my membership. And we have large and small businesses represented, and manufacturers. And as I said in my testimony, I think you certainly understand, and others do as well, that building strong digital rules is really across the board, not just about big tech. It is across sectors, across industries, and so that is what I was going to ask your forgiveness for, if I could divert to that for a moment.

But back to small business. I think that it is very clear that I know that the Commerce Department does a good job of providing information to small businesses to help them export.

I think there needs to be a lot more of that. I think small business needs to be provided with digital tools. I know certainly, among my members, there is a lot of that going on, where they have facilitator labs for start-ups and small businesses where they give them digital tools, whether it is AI, use of platforms, other digital technologies, cloud technologies. But I think there needs to be more of that from the government, as well as the private sector, maybe in public-private partnerships.

To answer your question about what specifically should be included in IPEF, for example, we think that it is very important that there be a provision where countries commit to the importance of providing those tools, digital tools, to small business, and capacity building in particular. Certainly the United States is very important, but also in IPEF countries.

And so, I think that that alone would be maybe the most helpful thing that could be done for small business in terms of specific provisions that could be added in IPEF, and also just general capacity building that I know CSI member companies are already doing in the U.S., but also in IPEF countries.

Senator CARPER. All right. Thank you.

The same question for Dr. Meltzer. What resources can better help small businesses to participate in the digital economy? And how can digital trade rules facilitate new export opportunities for both small and medium-sized enterprises?

Dr. MELTZER. Senator, thank you for the question.

Let me just go directly to the question of the digital trade rules. I think it is really worth noting that, in many respects, these rules are perhaps most important to small businesses, because the reality is that, at the end of the day, a lot of large businesses can manage the frictions and the costs, and they can locate facilities in countries where they may need to, but it is just not an option for small businesses.

And so a lot of the ways that the digital trade rules minimize transaction costs and make e-commerce particularly seamless are really the key benefit for them. I think about these in three buckets. I mean, one I would think about is those that facilitate e-

commerce. And there are some that have been around for a while but are really quite essential, like recognizing e-signatures. You cannot do a contract if that is not recognized in both countries. Issues around digital authentication and digital ID are new developments that also allow one to basically have a more seamless kind of person-to-person interaction online.

The *de minimis* outcome in USMCA which raised that in Canada and Mexico to facilitate e-commerce exports to these countries—there is a whole range of *de minimis* levels globally that we could look at trying to kind of find some agreement on, and just the nuts and bolts of the way Customs procedures work, and so forth, which is sort of the old work of trade policy, which is actually still relevant for e-commerce, because we are doing a lot of digital services online. We are also doing a lot of goods purchases online that still have to go through the typical trade channels. But making sure they fit for these kind of small business transactions is important.

Another one I would mention is around interoperability. The U.S.-EU Privacy Shield 2.0 is one that has gotten a lot of attention because of its impacts on Facebook, but it would have had enormous impacts on a whole range of small businesses if small businesses that were selling in to Europe were unable to collect personal data once they made their transaction.

So ensuring that, despite differences in regulations, data can flow freely, personal data can flow freely but remain protected, I think is a key thing that digital trade rules can continue to address, and that will have a big impact on small businesses.

And finally, we have all talked about data flows, but I mentioned in my written testimony and my oral testimony the importance of sort of platform-solving for the barriers that allow small businesses to become exporters. The data flow piece is actually the key there as well.

Senator CARPER. Thanks for those responses.

Ms. Bliss, at one point in time when he was responding, I was watching you, and you were vigorously nodding your head, and I thought, "Maybe I should call on her again." So, do you want to jump in and add something?

Ms. BLISS. Yes. I totally agree with what Dr. Meltzer described, and I am so glad that he mentioned trade facilitation, because that is another really important piece. But I also want to mention that I think a permanent moratorium on e-commerce duties is also critical, especially to small business, because that is something that can definitely hurt, particularly if there was retaliation, if it were to lapse and not exist with respect to small business, both exporting and importing.

So I just wanted to add that one as well.

Senator CARPER. Good. I am glad you did.

Mr. Feith, do you want to opine on this one?

Mr. FEITH. No, sir.

Senator CARPER. All right. Maybe I will give you another shot at a different question. This one deals with bolstering our cybersecurity and our digital infrastructure.

Digital infrastructure, including things like broadband, like data centers, like physical input, like semiconductors, have become critical to global trade, and have been for some time.

What vulnerabilities currently exist related to digital infrastructure? Talk about some of those, and how can we safeguard these resources—or maybe better safeguard these resources in order to protect the cybersecurity of American workers and our businesses?

Mr. FEITH. Well, thanks, Senator. It is a huge subject, and I will try to give you a limited answer. I think that we have seen a lot of really important action on recognizing the China-related threat in cyber-space generally, around things like the theft of intellectual property, say over the last decade, the threat that relates to telecommunications infrastructure in the U.S. and around the world, especially over the last 5 years or so. The understanding of what Huawei and ZTE and others mean—we have seen steady action from parts of our government that are responsible for those areas. We still need more of it, but we have seen at places like the FCC, the Federal Communications Commission, over the years, including just last week, a lot of effort to sort of gradually and increasingly restrict the ability of Chinese companies, subject to Chinese Communist Party influence and control, to be present in the hardware and software of the U.S. telecommunications infrastructure.

One thing that I would note, though, that is really interesting and kind of emergent about what this means in our consumer economy—but also in our national critical infrastructure—is things like drones and surveillance systems and cameras.

Some of these areas are, in a sense, uncovered by our traditional regulatory approaches. And so on drones, you have had this interesting and rather frustrating scene over the last several years where various parts of the U.S. Government—DHS, the Pentagon, and others—have put out statements that relate to the fact that these Chinese drones pose these major data-integrity concerns because of the complete ability of the data to be subverted by Beijing and used for hostile purposes.

But the statements from DHS, for example, are just advisory; useful and educational, but not really restrictive when it comes to what State governments or local law enforcement or power grid operators do when it comes to procuring drones.

Some of those DHS advisories succeeded in getting operators of power grid infrastructure, for example, to get rid of their Chinese-procured drones. But others did not get the message, and the message was just advisory. It was not mandatory. That sort of thing is present broadly throughout. And there are parts of the picture, such as the autonomous transport piece and the digital mapping piece, that appear to have gone basically entirely unremarked on, even by advisory statements from the U.S. Government, because we are still catching up with this issue.

So we have an issue where the leading autonomous transport companies in the country, doing really advanced things in California and Arizona and elsewhere, are in many cases deeply tied to financing and engineering and other connections to China—to the Chinese state, to the Chinese military—and yet they operate freely here. They operate without restriction when it comes to the sharing of U.S. road and port and other critical infrastructure digital mapping data, internationally back to engineering fleets in China. And all of that would seem to pose really very significant

risks in the sort of cybersecurity and critical infrastructure areas that you have asked about.

Senator CARPER. Good. Thank you. One last question.

My last question, and I will just telegraph this, but I am going to ask you a number of things. A number of times I will ask witnesses what should we do on this issue or that issue? I am going to ask you to give us one example of something we should *not* do as we go forward. Is there something we should not do? Okay, so just be thinking about that.

Okay, my question, my next question is of Mr. Woodall. Mr. Woodall, where are you coming to us from today?

Mr. WOODALL. In Washington.

Senator CARPER. Oh, good. You seem close; I can feel that. But anyway, whether you are in Washington, DC or Washington State, we are delighted to have you join us. How long have you been involved with the AFL–CIO Technology Institute?

Mr. WOODALL. For about a year.

Senator CARPER. Okay. Did you start right out of school? [Laughter.]

Mr. WOODALL. Yes, but not here. I have been working on public trade policy for decades.

Senator CARPER. Really? Okay, well good.

My question, serious question, is, as the use of digital technology grows, and as it evolves, it is critical that American workers feel the benefits of these innovations in a couple of ways. One would be through better jobs, and the other would be better wages, higher wages.

My question would be, how can digital trade cooperation in investments and in our workforce help ensure that American workers develop the kinds of skills that are needed for success in the digital economy? I visited businesses large and small a lot when we were on recess for several weeks earlier this month, and almost every day when I visited businesses large and small, I would ask them, how are we doing? How are we doing, we in Congress, in the State of Delaware, and what can we do to help? Actually what I heard more than anything else was, we just need people to come to work, people who are trainable, with the requisite skills, who are trainable for additional skills, added additional skills. That is what they said that they were looking for and needed. So I am focusing right now on that.

But my question, how can digital trade cooperation and investments help ensure that American workers develop the skills needed for success in the digital economy?

Mr. WOODALL. I think obviously, investment in workforce is critical for the next generation of technologies. This is the sort of discussion that is going on around the CHIPS and Science Act, and in other parts of the administration's agenda.

We have been very involved to make sure that the jobs that are created are good union jobs with good pay, and provide opportunities for advancement. We are very supportive of that.

I think what we are concerned about in the digital trade arena is the extent to which some of these technologies are really corrosive on workplace conditions and workplace fairness and erode workers' income. And so we have seen this with a lot of the algo-

rithmic management issues, and we are very concerned that it will be difficult to address things like workplace surveillance, the unfairness behind algorithmic management that workers face every day in the workplace. And frankly, much of this surveillance is off the job as well.

So it needs to be a situation where there is enough domestic governance space to protect workers from the downsides of the digitization, as well as provide opportunities for workers going forward in real workforce development that centers workers in that process.

Senator CARPER. All right; thanks. Do any other witnesses want to comment on that? Ms. Bliss?

Ms. BLISS. Mr. Chairman, I would just add that I think that one of the things that we have certainly endorsed and think is important is that there be a provision included in the new digital piece of IPEF—and in other U.S. initiatives—that addresses AI principles, including respect for human-centered values, which is certainly one of the OECD AI principles that we think is very important and could be helpful in addressing concerns about things like abuse of AI.

Senator CARPER. Thanks.

Mr. Feith, anything else you would like to add?

Mr. FEITH. No, sir.

Senator CARPER. Dr. Meltzer?

Dr. MELTZER. Just building on Christine Bliss's point, the White House released a blueprint for AI—human rights and AI—and I think this would be an excellent starting point to think about including in the digital trade agreement, because it would certainly reflect U.S. values, and I think it would get at a lot of the concerns that have been expressed today about ensuring that AI is used consistent with human rights as well as labor standards.

Senator CARPER. Mr. Feith, do you agree with that?

Mr. FEITH. Yes, Senator.

Senator CARPER. How about Ms. Bliss? Do you agree with that?

Ms. BLISS. Yes.

Senator CARPER. All right.

I told you I was going to ask you about any advice of what not to do on this front, and we would welcome that.

Mr. Woodall, if you do not mind, I am going to ask you to respond to that question first. I am not asking you to advise us in Congress what we ought to do, but what are we not to do, to be careful to avoid? Please, Mr. Woodall?

Mr. WOODALL. Certainly, I think there are a lot of things to be careful to avoid; I have talked about some. I think one area to consider avoiding is sort of blanket exclusions. And I would recommend something that would exclude personal vulnerable data and critical infrastructure from the data flow and data localization commitments that we have seen in other digital areas.

I think these are areas where there is broad consensus that there needs to be more protection, and so we should sort of not include that.

Senator CARPER. Dr. Meltzer, what should we avoid doing?

Dr. MELTZER. One comment about maybe the politics, which is not for me to manage, but avoid this becoming a partisan issue. I

think it has a huge economic value across the U.S., and we should be able to get behind this. But I think specifically, we should avoid walking away from anything that would dilute the commitment to data flows. I think the thoughts on the exceptions are really crucial here. It is really where the battles are being waged between maximizing the economic opportunities and providing the regulatory space for governments to keep doing what they need to be doing. And I think it is really important that we get that bit right.

Senator CARPER. Senator Cornyn, who is the ranking member on this subcommittee and was the chairman—we are glad to work across the aisle. And we do not see these as partisan issues. And Todd Young, Senator Young, who was here, feels very much the same way, and that is the way I like to operate.

And I get to chair the Committee on Environment and Public Works, and a lot of the big pieces of the bipartisan infrastructure bill came through our committee, which was adopted unanimously in our committee, and later by overwhelming margins in the Senate.

We have reported out big pieces of the Inflation Reduction Act, big pieces including methane reduction programs, unanimously, and later reported out unanimously the Water Resource Development Act, which will be before the Senate probably later next month.

A lot of folks across the country have worked together, and I am just here to tell you that a lot of times we do not get on television much when working together, but it is the glue that holds our country together, I think.

With that, my last question: is there a question that you maybe thought you would be asked, that should have been asked, that was not asked?

Dr. Meltzer, is there a question maybe you hoped would be asked that was not asked?

Dr. MELTZER. I think part of the piece here is the way the rest of the world is looking at what the U.S. is going to do in this space, and the perspective that the rest of the world has on the decisions that the U.S. makes. It is understandably a very domestically focused set of considerations at the moment, but the desire for, I think, U.S. reengagement on the digital trade piece in a lot of the Asia-Pacific could not be overstated.

They are dealing with the challenges from China in a geographically proximate way on digital regulation broadly, including across a whole set of issues. And I think this is one piece of what is really being asked for in terms of U.S. leadership that would be absolutely well received and welcomed in that part of the world.

Senator CARPER. Thank you.

Same question, Mr. Feith.

Mr. FEITH. Well, Mr. Chairman, I will go back to your previous question about what not to do, and I would offer a suggestion not to let these China data problems get so big they seem unfixable. TikTok was a lot smaller in its share of the U.S. social media market and in its cultural presence 2 years ago when the last administration attempted a ban. These things have grown bigger and more problematic very quickly.

We had an interesting discussion about the biodata question and whether too much has been transferred already, and whether it is too late. It would seem that it is not too late. But it can become so over time, the more that these sorts of problematic data relationships with China give Beijing leverage over us and box us in and limit our decision-making—and ultimately limit our sovereign ability to protect ourselves in this space.

Senator CARPER. Thanks for responding to that question as well.

Ms. Bliss and then Mr. Woodall, the same question of what you would like to have been asked but were not asked. Go ahead.

Ms. BLISS. Well, I think it was asked in some respects, but I think more about the importance of—and it is a corollary to what Dr. Meltzer raised about U.S. leadership, but at the same time what are the challenges that we face, particularly in IPEF, in getting not only our like-minded countries, but other countries that are now agreeing to participate in the trade bucket to get onboard with a high set of digital principles.

And I do think we face some real challenges there, particularly from countries like Indonesia and Vietnam. So that would be one question.

And the second thing I will answer to your previous question about what not to do is, I think it is absolutely critical that in IPEF—or any of our other initiatives with respect to digital—that we not go backwards, and that we build on what we have done. It can be improved. It should be added to, but we should not go backwards.

Senator CARPER. All right; that is good advice.

Okay, does anybody have a last thought? Mr. Woodall, anything else you want to add or take away?

Mr. WOODALL. No. I mean, I expected to sort of be asked about the ephemera of digital affecting real workers' lives, and I think there is a recognition that there are real challenges workers face because of the digitization, and we need to deal with that in more worker-centered digital trade provisions going forward.

Senator CARPER. Not everybody who answers the question leads with the word "ephemera," so thank you for that addition.

I think that is pretty much it. I just want to close with "thank you." I want to thank each of you for taking time to join us in person, or virtually from not too far away here in Washington. Thank you for what you do with your lives and for what you do for our country, directly or indirectly.

I want to thank Senator Cornyn, with whom I'm proud to lead this subcommittee. In fact, we have worked on a lot of issues, including some of the issues when the gun safety legislation was adopted several months ago. But we look for opportunities to work together. I have great respect for him and his staff, and I also appreciate very much the efforts of Senator Todd Young and the opportunity to partner with him.

And I would say to my own staff and other members of the staff, including the majority and minority staff of the full committee, how much we appreciate their working with us as we put together this hearing.

I have a script here that tells me—it gives me how many days my colleagues have to submit their questions for the record, and

they do not have much time. For the Senators who wish to submit questions for the record, those questions are due 7 days from today. That is a pretty quick turnaround. Our witnesses, however, will have 45 days to respond to any questions for the record.

So that should put us through, I think through December, through the holidays, and maybe into the beginning of the new year. But if you receive those questions, just try to get them back to us before too long.

And with that, I think this is a wrap. Thank you all. You are dismissed. Thanks so much.

[Whereupon, at 5:05 p.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF CHRISTINE BLISS, PRESIDENT, COALITION OF SERVICES INDUSTRIES (CSI)

Mr. Chairman, Ranking Member Cornyn, and members of the subcommittee, I appreciate the opportunity to appear before you today to discuss the benefits of digital services trade to businesses both large and small as well as workers and consumers across the economy. My name is Christine Bliss, and I am the president of the Coalition of Services Industries, a nonprofit trade association that represents U.S. services firms on services and digital trade issues. Our members include companies that provide distribution, logistics, financial services, professional services, and information and communication technology services. CSI members also include manufacturers of consumer technology, telecommunications equipment, and health and nutrition products. Our members both deliver many aspects of their services digitally as well as rely heavily on software and digital technologies in their business operations. CSI member companies operate in all 50 States and over 200 countries and territories.

Too often the discussion of the digital economy is narrowly and mistakenly viewed as an issue that only relates to and benefits large firms in the information and communication technology sector. In fact, it is essential to the health and future of companies both large and small in sectors throughout the economy: manufacturing, agriculture, health, education, environment, transportation and logistics, communications, finance, distribution and media and entertainment, to name just a few. It is a major source of existing and future U.S. jobs and growth fueled by U.S. global competitiveness.

To ensure that our economic growth is robust and that its benefits extend to all Americans, especially small firms, women- and minority-owned businesses, and workers and their families, it is vital that the U.S. not only ensure that its domestic infrastructure and industries are strengthened through measures such as the CHIPS Act, it must also address the threat to U.S. global competitiveness arising from growing digital protectionism and fragmentation. That is why it is more important than ever that the U.S. build strong binding, enforceable digital disciplines, remove discriminatory digital trade barriers, and promote greater inclusivity in the global digital economy by fully engaging with trade partners in the Indo-Pacific, UK and Europe, Taiwan, North America, Africa and Latin America, as well as the WTO and forums such as APEC.

CSI believes that promoting strong digital disciplines and greater inclusivity are complementary goals. Working together, Congress, the administration, business, labor, environmental groups, and other stakeholders in this new piece of the economy have a unique opportunity to develop policies that will shape the direction and growth of digital trade for years to come.

WHAT IS THE DIGITAL ECONOMY?

At its core the digital economy is powered by its basic communications network of fiber-optic cable, computer chips and other technology, software and services that create the Internet, and its ever-evolving platforms that enable data to carry information across the Internet and be used in myriad products and services. We carry on our lives via the digital economy from texting colleagues and friends on our mobile phones, working or shopping online on our laptops, to the factory floor from design, to construction and assembly of goods including the sensors that expand the

capabilities of those goods. Autos, tractors, planes, and everyday consumer products are produced using advanced manufacturing technologies that rely on data analytics, artificial intelligence, and cloud services where data may be stored and processed. Digital technology monitors the safety and operation of the planes we fly and the cars we drive. Digitally enabled tractors allow farmers to test soil quality or the cloud technology they use to time when to plant crops, digital technology helps farmers take care of their animals from herding, to reproduction, to detecting illness. Cross-border exchange of research and design facilitates development of computer chips and sharing of the latest medical research on critical new vaccines—this is just a fraction of the digital economy.

The digital economy is also playing an important role in addressing climate change through encouraging reduction of carbon emissions, and facilitating response and relief in instances of natural disaster. And along with greater efforts to expand broadband capacity, it is extending the reach of services available to underserved communities, particularly in areas such as health, education, financial services, and job opportunities in those sectors. Just think of how this committee was able to continue its work through the onset of the COVID–19 pandemic by working remotely, as were businesses, and schools and countless other examples.

As explained below, one of the greatest impacts of the digital economy is in helping small businesses establish and extend their reach into domestic and global markets.

ECONOMIC IMPACT OF DIGITAL ECONOMY

It is important that Congress and the administration focus on the impacts of the digital economy on American business and workers as it is a burgeoning source of economic activity, growth and jobs. According to the Commerce Department, in 2021, the digital economy generated $3.7 trillion in gross output, over 10 percent of total U.S. GDP.[1] Digital gross output increased by 9.8 percent in 2021, compared to 5.9 percent for the economy overall. The digital economy is also an important provider of jobs in the United States. In 2021, 8 million workers owed their jobs to the digital economy. An increasing percentage of U.S. jobs generally require digital skills. These skills are not needed just for professional level jobs. High school educated individuals are able to obtain certification that allows them to acquire needed skills in areas such as IT network building.

BENEFITS OF DIGITAL ECONOMY

The digital economy has been a key source of resilience for the United States throughout the pandemic, getting businesses—especially small businesses—and households through a challenging period.

Facilitating Social and Economic Resilience During the Pandemic

- Millions of workers had to figure out ways to work or go to school from home, and the Internet and other digital services made that possible.
- Digital services enabled hundreds of thousands of small businesses to become digital virtually overnight, sustaining their businesses through the pandemic. One-third of small businesses state that they would not have survived the pandemic without access to digital tools.[2] Just one example is **Freaks and Geeks LLC in Denton, TX,** where Alex Featherstone reported, "COVID forced us to shut down our physical store. Without any foot traffic to our store, we were not making a profit large enough to pay our store's rent and eventually we were forced to sell. Facing the death of my business, I decided to give eBay a try. eBay gave us a place to transfer all of our retail and keep our business alive. Thanks to the growth we have experienced on eBay, we will be able to buy another physical location once the pandemic ends."[3]
- Financial services firms made it possible for people to bank from home at the same time banks developed new digital technologies to assist the unbanked

[1] This and subsequent data reporting the importance of the U.S. digital economy are from the U.S. Department of Commerce, Bureau of Economic Analysis, "New and Revised Statistics of the U.S. Digital Economy, 2005–2021," *https://www.bea.gov/data/special-topics/digital-economy.*

[2] Connected Commerce Council, "Digitally Empowered," *https://digitallyempowered.connectedcouncil.org/.*

[3] eBay, "United States Small Online Business Report," May 2021, *https://www.ebaymainstreet.com/sites/default/files/policy-papers/2021%20Small%20Online%20Business%20Report.pdf.*

and facilitate government subsidies and direct payments to the American people. They also supported thousands of companies in getting PPP loans.
- Digitally connected supply chains eventually enabled manufacturers to restock their customers. Transportation and warehouse workers kept supplies moving, particularly of PPE goods needed to fight the pandemic.
- Cloud services—like the open industrial IoT, advanced analytics and AI provided by one U.S.-based cloud services provider—were an important way in which many manufacturers were able to address issues to their business end laid bare by the pandemic. Currently, 96 percent of manufacturers use cloud technology or plan use it in the near future.[4] Additionally, by the end of 2021, 90 percent of all manufacturing supply chains will have invested in the technology and business process necessary for true resiliency, resulting in productivity improvements of 5 percent.[5]
- Cross-border sharing of research and data supported the development of vaccines. The health-care industry pivoted to telemedicine. For example, companies like **Now Optics** *(https://nowoptics.com/our-journey/)* in **Indiana,** now provides virtual eye exams to customers across the United States, with customers more comfortable with telemedicine as a result of the pandemic.[6]

Helping Small Business Start-Ups Succeed

- **Olaris,** a women-owned life sciences lab in **Boston, MA,** with the help of AI technology has developed a non-invasive kidney transplant test. This small group of scientists was able to build an Internet platform to study the role of metabolics in the early detection of cancer.
- **Honest Jobs, a Denver, CO**-based small business founded by a former prison inmate, was able to create a platform using assistance in coding and use of cloud technology providing an employment network for ex-convicts trying to enter the workforce.
- **Marketing for Greatness, a Cedar Park, TX**-based marketing consultancy, was founded by Jessica Santos, a then-new mother. Transferring her legal and accounting skills to the digital economy, Jessica launched her own digital marketing firm and led the international expansion of a Fortune 500 company while working from home and raising four children.
- **Fraud.net,** a women-owned fraud prevention platform in **New York,** offers an end-to-end fraud management and revenue enhancement ecosystem specifically built for digital enterprises and fintech globally.

In many cases, the introduction of new digital goods and services into our daily work and home activities over the last 2 years has permanently changed the way we work and play.

DIGITAL SERVICES TRADE

As members of the subcommittee know so well, the U.S. economy depends on international markets. You know the statistic: more than 95 percent of the world's customers live outside the United States. Reaching those customers by exporting American goods and services now almost universally entails a cross-border digital services trade component.

- Manufacturers communicate with international customers via email and track deliveries over the Internet. U.S. manufacturers rely on services like finance, marketing, payments, insurance, and logistics to ship their products to international markets, all of which are digitally enabled in important ways.
- Small businesses use e-commerce to reach customers across the globe. eBay reports that ". . . eBay-enabled small businesses in every State have been engaging in global trade at a scale once reserved for the very largest corporations. The numbers are striking: a massive 96 percent of eBay-enabled small businesses in the United States export—a rate of exporting that dwarfs that of traditional businesses. . . . The ability of small, independent businesses to reach consumers anywhere across the globe has helped foster enterprise

[4] "Managing Application Development: The manufacturing perspective," Economist Impact, April 16, 2019, *https://impact.economist.com/perspectives/technology-innovation/managing-application-development-manufacturing-perspective.*

[5] IDC Futurescape: Worldwide Manufacturing 2023 Predictions, *https://www.marketresearch.com/IDC-v2477/IDC-FutureScape-Worldwide-Manufacturing-Predictions-32554203/*.

[6] Bill Briggs, "Vision quest: How Now Optics is delivering virtual eye care to millions of patients," April 14, 2021, *https://news.microsoft.com/transform/vision-quest-how-now-optics-is-delivering-virtual-eye-care-to-millions-of-patients/*.

growth in rural and more diverse counties, places that too often otherwise suffer from economic stagnation."[7]

- Engineers, architects, and accountants all benefit from being able to provide services such as design or financial consultations and send drawings internationally over the Internet without having to establish a foreign presence.
- Retailers process payments from customers both in the United States and abroad using online payment transaction services offered by American payment networks. Online access to this financial service is particularly important for enabling small retailers to service international customers.
- Insurance, shipping and other firms are increasingly using Blockchain ledger technology to keep real time track of accounts and transactions, increasing reliability and security of customer accounts for information.
- Tourists and business travelers book transportation and accommodation services over the Internet.
- Transportation services providers track the arrival and departure of ships or airplanes containing U.S. exports or imports in real time using GPS and other transportation management software.
- Small computer application developers and content creators, typically sole proprietors or small businesses themselves, benefit by expanding the range their sales into foreign markets via the Internet.

Selling goods and services to the world using digital trade supports American manufacturing, farming, and services creation and the millions of jobs associated with that trade activity. This is not just about promoting the interests of high-wage workers at large U.S. services and digital firms and other professional workers; it is also about creating new opportunities for the 52 million U.S. workers in services occupations earning middle-class wages.[8]

IMPORTANCE OF PROVIDING DIGITAL TOOLS TO SMALL BUSINESSES

Digital tools—*e.g.,* access to broadband, Internet platforms, and the latest digital applications in the cloud—are also vital to micro, small, and medium-sized businesses which increasingly depend on them to expand their domestic and international customer base. A study that surveyed U.S. small businesses found that 92 percent that export use digital tools such as online payment processing tools, online productivity tools, e-commerce websites, online marketing and other tools.[9] That same study found that exporting accounts for a growing share of small business services firms' revenues, reaching 25 percent in 2018, and nearly 6 million export-related jobs nationally. Particularly during the pandemic, Internet platforms afforded small businesses new opportunities to offer their goods and services globally, and software and services enabled small businesses to operate more competitively and efficiently.

Just one example is **Cloud to Street,** a **NYC**-based small women-founded and -owned business that uses digital tools to monitor, map and analyze floods and flood risk in the most climate-vulnerable communities around the world. Cloud to Street uses global satellites and remote sensing AI to monitor risk and detect floods in real time. This unique technology requires zero ground equipment and provides governments and communities with accurate and trustworthy flood monitoring in almost 20 markets worldwide.[10]

Digital tools are of particular importance to women-owned small businesses. A Visa Economic Empowerment Institute survey found that newer firms are increasingly "born digital and newly established women-led small businesses are particularly highly digitized: strong majorities use online stores and some forms of digital payments, including mobile payments, QR codes, established e-commerce payment providers, and new entrants in the payment space."

---

[7] eBay, "United States Small Online Business Report," May 2021, *https://www.ebaymainstreet.com/sites/default/files/policy-papers/2021%20Small%20Online%20Business%20Report.pdf.*

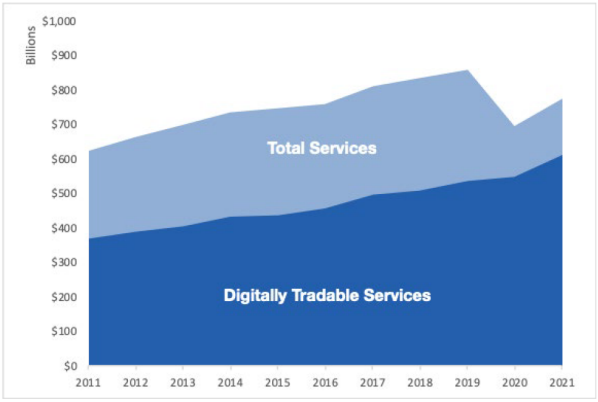
[8] CSI, "White Paper 1: Services and Digital Trade Are Critical to U.S. Competitiveness and Middle-Class Job Creation," *https://uscsi.org/wp-content/uploads/2021/10/CSI-White-Paper-1-Services-Dig-Trade-Comp.pdf.*

[9] United States Chamber of Commerce and Google, *Growing Small Business Exports: How Technology Strengthens American Trade,* October 2019, *https://www.uschamber.com/assets/archived/images/ctec_googlereport_v7-digital-opt.pdf.*

[10] Asia-Pacific Economic Cooperation, "From Platforms to Payments," Small and Medium Enterprises Working Group, 2022, *https://globalinnovationforum.com/events/apec-workshop-sme14-2019a/.*

The particular importance of digital trade during the pandemic is clearly illustrated by U.S. export data. Nationally, services exports remain below their 2019 peak. As shown in the graph below, the decline is wholly due to a sharp decrease in services provided to foreigners that typically are conducted in person. For example, U.S. exports of personal travel services declined by $88 billion (−78 percent) from 2019 to 2021 despite a slight rebound last year. Related export sectors fared similarly poorly, with large declines in U.S. exports of including business travel services (−64 percent), passenger fares (−68 percent), equipment installation and repair (−55 percent), and education (−13 percent).

U.S. Exports of Services, Digitally Tradeable Services, 2011-2021



Source: Trade Partnership Worldwide, LLC

Contrast that with exports of digitally enabled services that have been especially strong during the pandemic years. Digitally traded services exports increased by $74 billion (+14 percent) from 2019 to 2021. In fact, U.S. exports of digitally traded services have increased every year since 2011. Between 2019 and 2021, there was strong growth in U.S. exports of purely "digital" services such as customized software services (+27 percent) and cloud computing and data storage (+21 percent) as well as potentially digitally enabled services such as business management and consulting (+36 percent), financial management and advisory services (+29 percent), and legal services (+24 percent). Digitally tradable services have not grown enough to offset all of the COVID–19-related services export declines, but have certainly helped mitigate the damage.

The national trends extend as well to every U.S. State represented by a member of the trade subcommittee. According to estimates from Trade Partnership Worldwide,[11] every State saw increased exports of digitally tradable services between 2019 and 2021 but a decline in non-digitally trade services over the same period. In Chairman Carper's home State of Delaware, 2021 services exports exceeded their 2019 levels on the strength of digitally tradable exports including financial and insurance services. CSI prepared reports for each U.S. State detailing the importance of services and digital trade to each State; you can see the reports for each member of the trade subcommittee here:

Colorado	New Jersey
Delaware	North Carolina
Idaho	North Dakota
Indiana	Ohio

[11] Trade Partnership Worldwide, LLC, *CDxports* database, *https://tradepartnership.com/data/cdxports-and-cdxjobs/*.

Iowa	Oklahoma
Louisiana	Oregon
Maryland	Pennsylvania
Massachusetts	Rhode Island
Michigan	South Carolina
Missouri	South Dakota
Montana	Texas
Nebraska	Virginia
Nevada	Washington
New Hampshire	Wyoming

HOW CAN GOOD DIGITAL TRADE POLICY SUPPORT THE AMERICAN ECONOMY?

A robust U.S. trade agenda for services and digital trade is especially important for several reasons. First, it is an important means to promote democracy, freedom, access to information, and other core American values and press back against authoritarian regimes. Second it is an important avenue to redress barriers to digital services trade by ensuring non-discriminatory treatment of U.S. firms abroad and promoting enforceable harmonization of standards and disciplines with trade partners, whether those participating in the Indo-Pacific Economic Framework (IPEF), with the EU, UK, Taiwan, Kenya, the WTO and Latin America. Working to gain support of trade partners to promote democratic values and to achieve harmonization of disciplines and standards is important to ensuring their effectiveness. Third, digital trade is an increasingly important source of new jobs and we need to ensure that American workers—both blue and white collar—are ready to take advantage of those jobs. We also need to ensure the benefits of the digital economy and digital trade flow across the economy, especially to small businesses, and underserved communities.

PROMOTING AMERICAN VALUES

U.S. engagement on digital trade topics in bilateral, regional, and multilateral forums is a crucial opportunity for the U.S. to advance its vision of a free and prosperous trading regime anchored in American democratic market values. Other governments, including China, are actively working to shape the rules of the road for digital trade, often at odds with democratic values and the principles of openness and transparency. We also recognize the seriousness of national security concerns that China's digital policies have raised. In recent years, we have seen countries in political transition—like India, Brazil, Turkey, Vietnam, Pakistan, Indonesia, and Nigeria—rapidly adopt and adapt restrictive Chinese and Russian models of digital regulation, premised on sovereignty, censorship, surveillance, and security. The 2022 Freedom House report [12] notes that "governments are breaking apart the global Internet to create more controllable online spaces," with a record number of national governments blocking websites—mostly from sources outside of the country—with nonviolent political, social, or religious content.

U.S. engagement in negotiations to draft and implement international digital trade agreements is especially important to counteract China's protectionist and authoritarian whole-of-government approach to shaping the rules of the road on digital trade. In fact, China recently released its 5-year digital economy plan that clearly articulates its protectionist ambitions in this arena. China has also extended its influence on digital policies and standards at the World Trade Organization, the International Telecommunications Union (ITU), APEC and in the recently concluded RCEP, the world's largest trading bloc which accounts for 30 percent of global GDP, and does not include the U.S. China is also seeking accession to the CPTPP agreement—a high-standard trade agreement which the U.S. led and left—and the Dig-

[12] Freedom House, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet," *https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.*

ital Economy Partnership Agreement (DEPA). China's industrial policies and unfair subsidies benefit Chinese companies and unlevel the playing field for U.S. firms operating in the region, especially in the ICT sector. To be truly effective we need to gain the support of our trade partners in engaging in this effort.

ADDRESSING DIGITAL BARRIERS AND CREATING EFFECTIVE DIGITAL DISCIPLINES

We need to address the very real threat of increasing discriminatory foreign barriers to services and digital trade. As a primary example, data localization and data residency requirements are proliferating. Countries around the world—including some U.S. trading partners—are passing increasingly restrictive digital rules that disadvantage U.S. companies. For instance, the EU regulatory agenda includes policies such as discriminatory digital taxes and discriminatory cloud cybersecurity restrictions that undermine the ability of U.S. firms to access the EU digital market on an equal footing. These depart from a shared principles-based approach to regulation. We hope the U.S. Government will press the EU to provide clarification on compliance with the EU's Digital Markets Act and Digital Services Act. Both are sweeping pieces of legislation with complex requirements, and it will be important to ensure they are not implemented in a discriminatory or unduly burdensome manner.

This is a time when like-minded partners with shared values should be standing shoulder-to-shoulder to defend basic democratic values through a rules-based trade system that adheres to long standing norms of non-discrimination and openness.[13] Instead, such measures, particularly when imposed by allies, can undermine technological cooperation between trading partners. In the meantime, countries with authoritarian tendencies and with weak legal systems and rule of law are beginning to copy and further misuse these regulatory templates that undermine a transparent and non-discriminatory rules-based system for the global digital economy.

These not only pose major trade barriers to U.S. exports, but they also enable increased authoritarian influence, censorship and surveillance, while leaving networks vulnerable to cybersecurity risks and malicious interference. The Organisation for Economic Co-operation and Development (OECD) found that the services regulatory environment, particularly for foreign investment, became more restrictive in 2020 and the pace of tightening has accelerated.[14] The resulting "regulatory divergences" are raising cross-border costs as activities need to be aligned across multiple regulatory frameworks."[15]

CSI has provided the administration with further detailed recommendations *(https://uscsi.org/wp-content/uploads/2022/03/CSI-Calls-for-an-Ambitious-Indo-Pacific-Econom.pdf)* on these points, which we are happy to share with subcommittee members. We would however like to highlight a number of the areas we have included in our recommendations.

1. *Cross-border Data Flows and Prohibitions on Data Localization:* Cross-border data flows are the life blood of the digital economy and we believe that the cross-border data flow data and data localization provisions included in the bipartisan USMCA agreement should be included in other trade agreements. As noted above, the rise of data localization is pernicious and can enable authoritarian influence and censorship.
2. *Non-Discrimination for Digital Products:* U.S. digital services and content providers should be granted non-discriminatory treatment in foreign markets and allowed to compete on a level playing field with their foreign competitors. We oppose the imposition of discriminatory regulations which tilt the playing field in favor of domestic champions.
3. *Permanent Moratorium on E-commerce Duties:* This element should also be included to cover digital services and products as it was in the U.S.-Japan Digital Agreement. This provision is especially important for SMEs, for those involved in research and development in medical as well as commercial sectors and app developers who are frequently small businesses. Should the moratorium be allowed to lapse, exporters could face a chaotic Customs regime with potentially

[13] For specific CSI digital priorities with the EU, *see* letter from CSI to U.S. Trade Representative Katherine Tai, November 21, 2022, *https://uscsi.org/wp-content/uploads/2022/11/20221121-EU-digital-concerns-letter.TTC_.Amb_.-T.pdf.*

[14] Organisation for Economic Co-operation and Development, *OECD Services Trade Restrictiveness Index: Policy trends up to 2021,* February 2021, *https://issuu.com/oecd.publishing/docs/oecd-stri-policy-trends-2021.*

[15] Organisation for Economic Co-operation and Development, *op. cit.*

non-administrable Customs duties which would disproportionately hurt SMEs. Likewise, small businesses in developing companies would be similarly disadvantaged in terms of their access to software and app imports. Further, allowing the moratorium to lapse would be counterproductive to U.S. efforts to strengthen the domestic semiconductor industry, which relies on the ability to electronically transmit software and design information on a cross-border basis.

For similar reasons, we believe the WTO moratorium on e-commerce duties should also be extended at MC 13. We note in the WTO context that imposing duties on digital services could raise questions of GATS inconsistency. Although there is widespread support for continuation of the e-commerce moratorium among developing countries, including Malaysia, Thailand, Caricom countries, Nigeria, Mauritius, and even LDCs such as Zambia, some developing countries continue to want assurances about policy space to develop their digital industries. We believe these issues should be fully discussed in the WTO including alternative but WTO-consistent options to the imposition of tariffs.

In addition, imposing digital tariffs on e-commerce would essentially amount to a digital services tax and would be at odds with work towards implementation of an agreement at the OECD on a global minimum tax.

4. *Prohibition on Mandatory Transfer of Source Code and Algorithms:* We believe that this provision should also be included in any set of digital disciplines as included in USMCA and the U.S.-Japan Digital Agreement. This provision is an important protection against the unauthorized mandatory transfer of software source code and algorithms contained in such code. It does not however, prohibit a regulator or judicial authority from requiring a person to preserve and make available source code in instances where there is a specific investigation, inspection, enforcement action, or judicial proceeding.

5. *Greater Cooperation in Cybersecurity:* Provisions on cybersecurity cooperation that assume a "risk-based" approach should be included. Such an approach should be based on principles that are performance-based, rather than prescriptive; proportionate, rather than one-size-fits all; and that utilize industry standards.

6. *Adopting Best Practices in the Use of Artificial Intelligence (AI):* Use of AI is becoming an increasingly pervasive and powerful tool in expanding the digital economy. It is important that its use be subject to best practices, such as the OECD AI principles with the goal of eventually reaching agreement on harmonized AI disciplines that will ensure transparent, nondiscriminatory use of AI and protect against abuse.

7. *Applying Good Regulatory Practices to Digitally Enabled Services Standards and Conformity Assessment:* CSI believes that new disciplines applying good regulatory practices, transparency, and nondiscrimination to digitally enabled services standards and conformity assessment procedures would benefit all services exporters, but they would be of particular value to smaller services firms. SMEs are less equipped to bear the higher costs and greater trade frictions that have resulted from growing digital fragmentation. Indeed, OECD analysis has shown that in relatively more restrictive services markets, new exporters confront costs as much as 53 percent greater than those faced by incumbent exporters. Addressing barriers to services trade in the form of trade-restrictive standards and conformity assessments would especially benefit SMEs seeking to expand services exports. Increasingly, governments are implementing mandatory, unique national standards and technical regulations that are not interoperable and create barriers to trade and technological progress. The resulting fragmentation has created an urgent need to update the standards-related rule book for trade in digitally enabled services. It is important to note that trade disciplines on standards for digitally enabled services are highly compatible with a government's right to regulate and would in no way undermine that right.

8. *Provision of Greater Capacity Building and Digital Tools to SMEs:* Parties to any new digital initiative should agree to provide more assistance in the form of digital tools and capacity building to SMEs.

9. *Promotion of Worker Digital Upskilling:* Yet another way in which policymakers can support American workers is to collaborate with American businesses to ensure that our educational system is ready to train students with the required skills to meet the requirements of jobs needing digital competencies. As services and other jobs increasingly demand digital skills obtainable by both professionals and the high school educated, both government and industry must do

more to equip individual workers with the requisite training. A study by Brookings found that nearly two-thirds of the new jobs created between 2010 and 2016 required at least a moderate level of digital skills.[16] The same report found that nearly a quarter of workers were already engaged in occupations with a high level of digital content. It also concluded that holding education constant, workers with better digital skills tended to earn higher wages than those with lower skills. Government and companies should collaborate to improve education and training programs. For example—just one of many—is "Girls4Tech," Mastercard's signature education program, which was launched in 2014 to drive the interest of young girls in science, technology, engineering and math (STEM). The curriculum is designed to teach participants curiosity, develop an innovative mindset and take a smart approach to solving everyday challenges using technology. Ultimately, the program aims to help bridge the skill gap in the technology industry. Girls4Tech is tailored for girls ages 8–16 to encourage their interest in cryptology, digital convergence, algorithms, biometrics, AI, and more. Many others engage in extensive digital skills training program, for example CISCO offers certificate level training programs for high school graduates at community colleges. A catalogue of CSI member programs is provided here *(https://v8v669.a2cdn1.secureserver.net/wp-content/uploads/2021/10/CSI-member-workforce-dev-programs.pdf),* and we would welcome your engagement with us on ways to make these kinds of programs more broadly available to American workers.

In the IPEF context, CSI members understand that in order for the Indo-Pacific region to grow and thrive, workers, small businesses, institutions, and governments must have the knowledge and skills to participate in the digital world. To that end, CSI member firms have developed innovative programs and partnerships that promote women-owned small businesses, capacity building, financial inclusion and education, cybersecurity training, digital infrastructure development, and worker skilling. We would similarly welcome the opportunity to engage with Congress on ways to collaborate and integrate such programs in the IPEF.

10. Trade Facilitation Measures: Agreements that promote the implementation of measures that facilitate trade also benefit American workers and their employers. Many of those measures are digital in nature—*e.g.,* filing entry paperwork online, or even consistent online publication of current tariff schedules, regulations, and forms for customs clearance. The U.S. *de minimis* threshold must be protected along with other measures that reduce red tame for SME exporters and importers. In a similar manner, measures such as the General Product Safety Regulation, are of concern for small businesses selling to the EU. One study found that if all countries implemented the same trade facilitation measures currently employed in the United States, U.S. employment would expand by nearly 1 million jobs, of which 79 percent would be at small businesses.[17]

The IPEF discussions present an opportunity to address some of these problems. Deepening commercial ties with the Indo-Pacific region is key to U.S. services sectors, which are increasingly digitally delivered and a key enabler of Indo-Pacific trade in all sectors. In 2021 alone, the value of U.S. services exports to the Asia-Pacific region was $180 billion, of which $124 billion were digitally enabled services.[18] As more countries in the region develop regulatory regimes focused on the digital environment, an increasing number of them are using the opportunity to impose discriminatory protectionist measures. These policies include overly broad, arbitrary foreign investment restrictions, data transfer restrictions, targeted curtailment of U.S. market access, data localization requirements, cloud services barriers, nationality of ownership restrictions, quotas, and discriminatory standards, among others. A high-standard digital trade agreement in the Indo-Pacific with binding rules is needed to counter the promulgation of such discriminatory measures, which disadvantage U.S. workers and employers not just in the services sectors, but across the economic spectrum. We note that greater integration, cooperation, and high-ambition digital standards in the IPEF region is a key part of U.S. national security strategy as well.

---

[16] Mark Muro, Sifan Liu, Jacob Whiton, and Siddharth Kulkarni, Brookings, *Digitalization and the American Work Force,* November 15, 2017, p. 15.

[17] Gabe Horwitz, "Reducing the Red Tape Around Supply Chains," Third Way, July 25, 2022, *https://www.thirdway.org/report/reducing-the-red-tape-around-supply-chains.*

[18] Trade Partnership Worldwide, LLC, *CDxports* database.

Longstanding trade principles of non-discrimination, transparency, openness, and interoperability should take center place in the trade module of the IPEF. It should also include a consultation mechanism and other means to raise member concerns and to hold members accountable. It is also critically important that these disciplines be legally binding enforceable. We also believe that these disciplines can be developed consistent with the long recognized trade agreement principle of recognizing the importance of respecting government's right to regulate.

We also believe that Congress has an important role to play in shaping these disciplines and that full and regular consultation and transparency must be a part of their development. In this regard support a bipartisan extension of Trade Promotion Authority.

CONCLUSION

Thank you for the committee's attention to these critical issues. We believe that creating strong disciplines on digital trade are important to promote job creation and competitiveness across all sectors of the economy and to advance American values abroad. We look forward to working with committee members and the administration to support this effort.

PREPARED STATEMENT OF HON. THOMAS R. CARPER,
A U.S. SENATOR FROM DELAWARE

Good afternoon. It's my pleasure to call this hearing before the Senate Finance Subcommittee on International Trade, Customs, and Global Competitiveness to order. Thank you to our witnesses for joining us to testify today. And I want to say a special "thank you" to our subcommittee's ranking member, Senator Cornyn—as well as Chairman Wyden and Ranking Member Crapo, and their teams—for working with both Senator Cornyn's and my staff to plan this hearing on digital trade.

Today's hearing will offer an opportunity for us to answer three central questions. First: what is digital trade, anyway? Second: why is it important to Americans? And finally: how can we work with our allies to strengthen our ever-changing digital economy? Today's hearing will also be the first Senate hearing in this Congress to specifically explore the importance of digital trade. I'm glad we can take this dedicated time, in a bipartisan way, to dive into this critical issue with leading experts across our Nation.

When I first started learning about digital trade, I quickly discovered it is necessary for us to better understand and appreciate how digital technologies and the Internet have transformed our economy. I'd like to take just a couple of moments to talk about this through an example that we have all come to know very well: smartphones.

Smartphones are everywhere in our society—nearly everyone I know has one, and it's almost impossible to imagine our lives today without them. We use them for everything: from checking work emails to logging into a Zoom meeting to purchasing goods from halfway around the world. Whether you're booking a hotel in Dover, DE or Dover, England, smartphones have made our lives more accessible to just about everything.

These are just a few examples in our daily lives that show how digital connectivity makes it easier, faster, and less expensive to trade goods and services across the globe. And this is all made possible because the Internet has made it easier for us to share information and data without geographic barriers. Without these tangible barriers, digital innovation has revolutionized nearly every industry across our economy, ranging from manufacturing to agriculture to financial services to e-commerce—you name it!

As a result, trading goods and services, with a lot of help from the Internet, has exploded in recent years. Just look at the numbers: from 2005 to 2019, real value added for the U.S. digital economy grew at an average annual rate of over 5 percent per year, outpacing the 2-percent growth in the overall economy each year. And the pandemic has spurred digital growth even more, with people staying home and turning to the Internet to access medical services, stream their favorite movie, or book that next vacation in the first State, another State, or around the globe.

And this growth isn't just benefiting consumers—it's also spurring job creation and enabling small businesses to thrive. With the digital economy, a small business

that sells jewelry in Delaware or Texas can now sell their products to anyone, anywhere in the world with ease.

However, it's critical that as we examine the importance of digital trade for our economy, we must also acknowledge how digital technologies affect our national security. Right now, we are witnessing a global battle over the values that govern the digital economy. Foreign adversaries like China are using digital technologies to advance authoritarianism and crack down on freedom of speech and human rights. They are working overtime to shape the digital economy in a way that threatens our democratic values and jeopardizes our national security.

Yet as Albert Einstein once said, "In adversity lies opportunity." And that's exactly what we have before us today: a real opportunity to set rules of the road for digital trade that reflect our values. Those words were true then, and are even truer today. So far, the U.S. has taken a leadership role through negotiating ambitious digital rules in the USMCA agreement with Canada and Mexico and through digital trade cooperation with Japan—but that's not enough. Our work cannot stop there.

That's why this past July, my staff and I worked closely with Senator Young and his staff and other members of this committee to introduce a bipartisan, bicameral resolution advocating for the United States to work with our allies across the globe to establish forward-looking global digital trade policies.

I'm also eager to work with U.S. Trade Representative Katherine Tai and the Biden administration to make progress on these important issues as they negotiate the Indo-Pacific Economic Framework and other economic engagements related to digital trade.

In that spirit, today I look forward to hearing from our esteemed panel of witnesses as they pull back the curtain on the importance of digital trade and how we can work with our allies to advance thoughtful digital trade policies. And with that, I'd like to turn it over to Senator Cornyn for his opening statement.

PREPARED STATEMENT OF HON. JOHN CORNYN,
A U.S. SENATOR FROM TEXAS

Thank you, Mr. Chairman, for organizing this hearing. It's been a pleasure as always working with your staff, and thanks to all of our witnesses for being here and sharing their expertise and knowledge. I like the three questions that you plan to ask or have teed up here. This subcommittee has consistently focused on the threat that China poses to our national security through its weaponization of trade, contrary to the international rules-based system that we thought they were joining when they became part of the WTO.

On that note, I want to express my concerns with regard to reports that our allies in Europe may retaliate for provisions of the recently passed Inflation Reduction Act. In the face of existential challenges posed by the Chinese Communist Party and its allies in the Russian Federation, a strong relationship with our partners in Europe is more important than ever.

Unfortunately, legislation passed on a purely party-line vote, like the Inflation Reduction Act, has moved us in the wrong direction. And I hope the administration will work to limit the trade ramifications from this bill with regard to Europe and our other allies. We all know that the results of protectionism helped put us into the Great Depression nearly a century ago, and we simply cannot afford to repeat it or get anywhere near it.

On this subcommittee, we've advocated for the U.S. to join the CPTPP, which was a mistake for us to walk away from in the first place. I was with Senator Hagerty, the former Ambassador to Japan, now a member of the U.S. Senate, and Senator Cardin, our colleague on the Finance Committee, in Japan recently. In every single meeting we had with our Japanese Government counterparts, they mentioned the TPP. And Senator Carper and I have written and spoken together on what a mistake it was for us to walk away from that. And my hope would be at some point we would get back in the game in Asia with the CPTPP.

Unfortunately, so far the Biden administration has refused to reopen negotiations on that agreement. So we need to look to sectoral-specific free trade agreements that focus, for example, on digital trade. This was also part of the conversation we had with Ambassador Emanuel in Japan when we were there. As each of our colleagues know, free trade agreements passed through Congress are insulated from domestic

political pressure. They provide long-term certainty for our businesses and reinforce the key economic relationships that we have with our friends and allies.

We've also focused on China's use of censorship as a barrier to digital trade in particular. We see today how China is weaponizing its digital infrastructure against its own citizens for simply protesting in the streets. One of the first tasks we should explore is how to define digital trade, which is the question Chairman Carper raised first—and appropriately so. For everything digital or virtual—from the cloud to artificial intelligence—there is obviously an underlying physical element. For digital trade, that medium is semiconductors, so maybe we should start by using that physical apparatus as a starting point for our discussions.

The second area we should explore is how digital trade agreements help to solidify our relationship with our friends and allies against the threat posed by the Chinese Communist Party. So I believe any digital trade agreement with our allies and partners should include provisions that incorporate disciplines on semiconductors as part of it. That includes things like coordination of semiconductor incentives, harmonization of our export controls with regard to China, and supply chain resiliency.

Finally, most importantly, we should find common areas of agreement amongst all stakeholders to include business, labor, and national security. That includes topics like preventing data localization and forced technology transfers. We should have free and open digital trade facilitation with clear rules of the road. For example, we should not be taxing electronic transmissions between our borders, or forcing data centers to be located in one nation or another. As with all issues pertaining to China, that will require a fair amount of discussion, debate, and even compromise.

So I look forward to hearing from our witnesses today, who represent a facet of each of those.

I'd like to welcome Mr. Feith for the national security perspective, Mr. Woodall for the labor community, Ms. Bliss from industry, and Mr. Meltzer from the think tank community that's important to give us the intellectual firepower we need to make good decisions here in Congress. So thank you all for being here today, and I look forward to hearing from you.

PREPARED STATEMENT OF DAVID FEITH, ADJUNCT SENIOR FELLOW, INDO-PACIFIC SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Chairman Carper, Ranking Member Cornyn, and members of the subcommittee, it is a privilege to appear before you today. Thank you for your invitation.

This hearing addresses digital trade, and I will focus my testimony on the national-security problems in this area posed by China—specifically, concerns about China's open access to American data.

I want to stress three points.

First: The importance of recognizing the China challenge. China is an outsize player in global digital trade flows. It is implementing aggressive strategies of data control, data exploitation, and data mercantilism. U.S. policy is not yet answering those strategies.

Second: The United States not only should work *overseas* to expand our digital trade arrangements, we also have urgent work *at home.* Our domestic task is to curb the massive unregulated flows of sensitive data to China. Our trading partners in Europe, Asia and beyond face the same challenge, even if some fail to recognize it.

Third: Immediate action can be taken in at least three areas: (a) to ban TikTok and the TikToks yet to come, (b) to begin controlling exports of Americans' biodata, and (c) to implement the so-called "ICTS" process endorsed by both the previous and current administrations but not yet in use to limit U.S. data flows to China.

THE CHINA PROBLEM IN DIGITAL TRADE

In our unfortunately polarized politics, it is an important sign of health that there is strong bipartisan support for countering China's national security threats. There is also bipartisan support for boosting U.S. digital trade links overseas.

The digital economy accounts for some 10 percent of U.S. GDP; digital trade contributes more to U.S. GDP than financial or merchandise flows; and digital trade

is growing faster than traditional trade in goods and services. There is particularly strong support for increasing such trade with the Indo-Pacific, where the United States has vital interests and strong allies and partners eager to work with us to prevent China from achieving regional hegemony.

But to set new global rules for the data age, and to compete with China, it is not enough to expand digital trade with friends. We also need to limit our digital trade with China. And we need to take action not just overseas but at home. Our challenge is how to begin placing national-security controls on data flows to and from China. We are late in addressing this challenge. If we don't do so soon, the national-security costs may be so high that they will far outweigh the benefits of any improvement in trade rules with our foreign friends. Our failures in domestic regulation may severely limit our ability to shape rules abroad.

A necessary first step is understanding China's approach to digital trade, which has long been far more strategic, mercantilist, and non-reciprocal than U.S. policy has recognized. It is a key element of China's national-security strategy.

For nearly a decade, Chinese leader Xi Jinping has declared that data in the 21st century is like oil in the 20th century: the critical input for fueling economic strength and national power. In 2013, he told his state-run Chinese Academy of Sciences:

> The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources for development and have the upper hand.

The analogy between data and oil later became something of a cliché in certain circles. But U.S. policy never recognized its logic. China's did.

The Chinese Communist Party developed a comprehensive strategy to control, accumulate, and exploit data. Data such as personal health records, personal genetic sequences, and personal online browsing habits. Data such as corporate trade secrets, corporate supply chain records, and corporate financial accounts. Data such as the photos, voice recordings, and mapping imagery pulsing through phones, drones, and smart cars all around the world.

Beijing recognizes that the competition for global influence in the 21st century will require protecting and harnessing such data to achieve commercial, technological, military and intelligence advantages. And that's what it is doing.

Beijing has built a latticework of laws and regulations to make the Chinese Communist Party the world's most powerful data broker. A set of laws implemented in 2017 gave the Communist Party unchecked access to private data on Chinese networks, whether those networks are in China or associated with Chinese firms such as Huawei overseas. Last year, Beijing enacted additional laws that go even further, demanding not just access to private data but effective control over it.

This has a huge impact on foreign firms operating in China. Not only must their Chinese data stay in China and be accessible by the Chinese state, but Beijing now demands control over whether those firms can send the data to their own headquarters; or to a corporate lab in, say, California; or to a foreign government that has made a lawful regulatory or law-enforcement request. Under Beijing's new laws, it may be criminal to comply with foreign sanctions against China that involve data. So if the U.S. Government, for example, wants to shut off banking or cloud services to a Chinese entity linked to human rights atrocities, a U.S. or other company can comply with U.S. law, or it can comply with Chinese law, but not both.

Boxed in by Beijing, Tesla, Apple, and others have opted to build dedicated Chinese data centers—sometimes in partnership with Chinese state entities, lest they lose access to the large Chinese consumer market and valuable manufacturing supply chain.

Beijing's bullying data rules inside China complement its longstanding efforts to buy, steal, and otherwise acquire data from outside of China. Beijing hacks foreign corporate databases. It runs "talent recruitment" programs at foreign universities and firms. It buys foreign companies. And it funds its own data-driven companies to conduct research, forge partnerships, win customers, and vacuum up data in open foreign markets like Silicon Valley, Boston, and Austin.

Beijing's data strategies also prize global propaganda, censorship, and influence, all to advance Xi's stated goal of winning the digital "public opinion struggle." Xi wants the Chinese Communist Party to have what he calls "discourse power," mean-

ing the ability to set and shape global narratives. Hence his aggressive regulation of the algorithms and other data technologies that power Chinese apps such as TikTok that are increasingly dominating the U.S. social media market. TikTok enables Beijing not only to harvest mass American data but to transmit favored messages, export censorship preferences, and potentially manipulate and mobilize Americans on a grand scale completely without precedent for a foreign power.

Beijing's approach is nakedly non-reciprocal. It relies on access to data from foreign countries while denying foreigners access to data from China. In China, Beijing controls the data of foreign companies. Outside of China, Chinese companies operate comfortably, creating and accessing valuable new data sets primed for easy transfer back to China in all manner of data-intensive fields—biotech, pharmaceuticals, medical devices, drones, autonomous cars and trucks, social media, digital payments, e-commerce, and more. These data flows to China contain massive quantities of information about American citizens, American companies, American government, and American critical infrastructure.

This is the stuff of digital trade. Yet there are effectively no rules governing any of it. There is nothing effective under the World Trade Organization or any U.S.-China bilateral trade accord, and not under U.S. domestic law either. The United States has no comprehensive Federal approach to data governance. Because of the nature of the internet—namely, that it was able to expand globally in a permissive environment, without any of the state controls inherent with traditional goods transported by truck or ship—digital trade (including U.S.-China digital trade) has remained fundamentally unregulated.

In this environment, for upwards of a generation, Beijing has been effective in designing a strategy of global data mercantilism: hoarding and controlling data for me, relinquishing and exposing data for thee. If the United States and our allies do not organize an effective response, Beijing will succeed in commanding the heights of future global power. Any new digital-trade arrangements we make with our partners would still operate in the shadow of a global digital-trade order that is open to fatal exploitation by Beijing.

THE DOMESTIC REGULATORY IMPERATIVE

The Biden administration has spoken about the importance of data in our competition with China. "Our strategic competitors see big data as a strategic asset, and we have to see it the same way," said National Security Adviser Jake Sullivan in 2021. But no visible strategy has emerged.

The U.S. Government has traditionally had no mechanism for limiting cross-border data flows, even on national-security grounds. Traditional national-security restrictions on commerce are designed to address other issues, and they have historically been narrowly scoped, consistent with important American traditions of limited government. The Committee on Foreign Investment in the United States (CFIUS) screens inbound investment. Export controls restrict outbound flows of U.S. goods and technology (and of some data, in limited cases). Procurement restrictions limit what Federal Government departments and agencies can buy.

But vast areas of economic life are largely or completely untouched by those tools—including the cross-border exchange of data by private companies, individuals, academic institutions, and State and local governments. When a U.S. hospital system wants to partner with a Chinese pharmaceutical or genomics company, or an American teenager wants to download a Chinese social-media app onto her phone, or your State government wants to procure Chinese drones to monitor the power grid or assist in law enforcement, the Federal Government has traditionally had no way to regulate such activity to protect national security.

Washington began to address this problem only recently, through the creation—at least on paper—of a new regulatory regime for reviewing cross-border data flows. Known as "ICTS" (for Information and Communications Technology and Services), this regime was established in the previous administration's waning days and maintained by the Biden team through a June 2021 executive order on "Protecting Americans' Sensitive Data From Foreign Adversaries." Under the ICTS process, a Commerce-led interagency panel can investigate, modify, block, or unwind data-related commercial transactions believed to present "undue or unacceptable risks" to U.S. national security.

This ICTS panel has authority across six sweeping sectors: critical infrastructure; network infrastructure, including satellites, wireless networks, and cable access points; data hosting, including services with the personal information of more than

1 million Americans; surveillance and monitoring technology, including drones; communications software, including mobile and gaming apps; and emerging technologies, including artificial intelligence and autonomous systems. These sectors touch nearly the entire modern economy.

But the ICTS process has not yet been put to use—not against Chinese access to U.S. data centers or biotech labs, not against Chinese drones with eyes on U.S. critical infrastructure, and not against other channels through which large volumes of sensitive U.S. data can flow to China.

Apart from ICTS, the Congress could of course consider legislative approaches. Various bills have been proposed to limit the ability of Chinese apps to operate and collect data in the United States, but without success.

Another idea is to create a new export-control category to restrict the sale of bulk personal data to certain foreign countries. This is the essence of the "Protecting Americans' Data from Foreign Surveillance Act" introduced in June by Chairman Wyden of this committee, with four Republican and Democratic cosponsors. But the fate of that bill is uncertain, and the issue of Beijing's data mercantilism was largely unexamined in the congressional work that resulted this summer in the CHIPS and Science Act.

Elsewhere on Congress's agenda, there is the risk that efforts intended to rein in domestic big tech platforms could end up imposing stricter standards on American firms than on Chinese ones. This would be perverse in terms of commercial competition and U.S. national security.

THE INTERNATIONAL PATH TO "DATA FREE FLOW WITH TRUST"

Also perverse is our longstanding failure to work with our allies (especially in Europe) to address China's digital-trade abuses as part of our international trade diplomacy.

Across effectively the entire era of digital trade, we have been at cross-purposes with Europe over data-privacy rules, while far greater data-related harms from Beijing have mounted. Chinese companies processing European data are in principle subject to localization and privacy-protection requirements under the European Union's General Data Protection Regulation (GDPR). But the EU has to date shown no great concern with mass data collection and exploitation by Chinese companies functioning as extensions of the Chinese state—especially compared with the EU's longstanding rage against U.S. big tech.

To be sure, there is a new test case involving TikTok. The Irish Government recently investigated the Chinese platform's data practices and sent findings to the EU Data Protection Commission. Brussels has yet to report back.

In the Indo-Pacific, the dynamic is more fluid. The 11-nation Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) includes high digital standards consistent with those of the U.S.-Japan Digital Trade Agreement (2019) and USMCA (2020), both of which were crafted with Beijing's abuses in mind.

Beijing prefers lower digital-trade standards, like those in the Regional Comprehensive Economic Partnership (RCEP) agreement, to protect its mercantilist and authoritarian interests. That is why it is now pushing to join both the high-standard CPTPP and the non-binding but potentially high-standard Digital Economic Partnership Agreement involving Singapore, New Zealand and Chile—to try to shape (that is, restrain) their standards from the inside. Beijing realizes that digital-trade flows are still overwhelmingly unregulated, and it wants to influence whatever might emerge to fill this international regulatory gap.

Important as it is, keeping Beijing from entering CPTPP against the rules is not enough. Fashioning a high-standard Indo-Pacific digital-trade agreement would be good. So would beginning to impose reasonable national-security restrictions on U.S.-China data flows, followed by consultations to encourage partners to do the same.

The concept that combines these two elements—digital-trade expansion with friends, digital-trade limitation with rivals—is what late Japanese Prime Minister Shinzo Abe called "Data Free Flow with Trust" (DFFT). We should maximize data trade with those we can trust and limit data trade with those we cannot. In other words, more data flow among democratic allies and other like-minded countries, and less data flow with China.

DFFT is a simple notion that will be hard to implement given China's size, strength, and deep integration into our digital economy and that of our allies. It is necessary, however. We are overdue in recognizing data as a strategic resource. Our responsibility now is to design a global digital-trade order that reflects democratic values and not Beijing's.

THREE IMMEDIATE OPPORTUNITIES FOR ACTION

U.S. legislators and policymakers can prioritize immediate action in at least three areas:

1. **TikTok—and the TikToks to Come:** As the Biden administration reviews TikTok via the Committee on Foreign Investment in the United States (CFIUS), Republicans Marco Rubio and Mike Gallagher have called for legislation to ban the app. Their approach could provide statutory authority to overcome the statutory barriers (namely the Berman Amendment to the International Emergency Economic Powers Act) that caused the previous administration's attempted TikTok ban in 2020 to fail in court. Democratic Senator Mark Warner (also on this committee) recently endorsed a TikTok ban in principle, calling the platform "an enormous threat."

   TikTok's fate is an acute test of Washington's seriousness about data privacy, counterintelligence, election integrity, and democratic sovereignty. No hostile foreign power has an entitlement to control a leading U.S. media platform. And keeping hostile foreign powers from wielding such influence is a safeguard of free speech.

   But TikTok's fate is also a test for other data threats looming on the horizon. TikTok parent Bytedance has a virtual-reality subsidiary, Pico, that wants to compete in the U.S. metaverse market soon against Meta and Apple. Fellow Chinese tech giant Tencent operates WeChat and other platforms in the United States. As long as such Chinese-owned and -controlled platforms enjoy unfettered access to U.S. consumers, Beijing will exploit that access for asymmetric strategic advantage.

2. **Biodata:** For all the controversy over TikTok and the obvious complexities in regulating a wildly popular platform, it is widely agreed that Americans should protect their health and genomic data, on grounds of personal privacy and national security. And yet U.S. law and policy have not yet risen to this challenge.

   The protection of biodata deserves to be at the top of Washington's tech-competition agenda. We have seen much commendable action in recent years on semiconductors, including initial moves by the previous administration, the CHIPS Act this summer, and the pending Schumer-Cornyn proposal to extend "section 889" Federal Government and contractor procurement restrictions to Chinese-manufactured chips. President Biden recently announced measures to promote domestic biotech and biomanufacturing, but there are no corresponding protections on biodata flows.

   Meanwhile Chinese pharma and genomics companies such as WuXi Apptec and BGI are expanding operations in the United States and partnering with U.S. hospitals and universities. These companies answer to Beijing's Party-state and military, part of Xi Jinping's growing military-industrial complex for precision medicine. As the University of Virginia's Aynne Kokas has written in an invaluable new book, China's access to U.S. health data, especially DNA, threatens harms "with multigenerational consequences."

3. **"ICTS" Implementation:** The new "ICTS" process may be the single best tool Washington has for addressing the multifaceted China data problem. It is vital, then, that ICTS get off the ground with appropriate staffing, funding, and authority. The administration may have most or all of what it needs to activate the ICTS, but some congressional action may be helpful, too.

   Consider the wide range of problems that ICTS could address, if appropriately used:

   - Data centers: The June 2021 executive order clearly threatened Chinese firms' continued access to U.S. "large data repositories," and Commerce reportedly subpoenaed several Chinese communications firms in early 2021. Yet no enforcement action has followed.
   - Drones: U.S. officials have issued years of warnings about Chinese drone giant DJI, which DOD recently added to a list of firms tied to China's mili-

tary. Yet DJI still dominates the U.S. commercial drone market. Another Chinese drone maker, Autel, is growing its U.S. sales while keeping a relatively low profile. Drones are within ICTS's mandate but they have not been the subject of any known enforcement action—or even investigation.

- Autonomous vehicles and digital mapping: Many leading U.S. autonomous transport companies rely on financing and engineering from China, while facing no restrictions on the export of sensitive data about U.S. roads and critical infrastructure. ICTS appears to have authority to stop this, but hasn't done so.

ICTS was designed to solve all of these cases. As with TikTok and biodata, addressing them would demonstrate prudent data regulation at home that could be a model for digital-trade policy promotion overseas.

China threats and digital trade are overlapping fields of bipartisan concern. The stakes are high. Immediate action is possible and would be valuable. The administration would benefit from congressional action, and the American people would appreciate the greater protection of their privacy and the strengthening of their national security.

Thank you for the opportunity to testify. I look forward to your questions.

*Center for a New American Security (CNAS) disclaimer: As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable Federal, State, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable Federal law. The Center publicly acknowledges on its website annually all donors who contribute, *https://www.cnas.org/support-cnas/cnas-supporters.*

PREPARED STATEMENT OF JOSHUA P. MELTZER, S.J.D., SENIOR FELLOW, GLOBAL ECONOMY AND DEVELOPMENT, BROOKINGS INSTITUTION

Chair Carper, Ranking Member Cornyn, and members of the subcommittee, thank you for the opportunity to testify today.

I am a senior fellow at the Brookings Institution, where I work on digital trade issues as well as on emerging technologies such as artificial intelligence.

Today I will focus my testimony on the opportunities of e-commerce and digital services trade for the U.S., with a focus on the opportunities for small and medium-sized enterprises (SMEs). I will also discuss evolving global AI regulation. In both these cases I will outline how digital trade commitments—whether in Free Trade Agreements (FTAs), Digital Economy Agreements (DEAs) or the Indo-Pacific Economic Forum (IPEF) negotiations, can support growth in e-commerce opportunities, in digital services trade and support AI regulation and R&D consistent with U.S. values and strategic objectives.

WHAT IS DIGITAL TRADE?

There is no globally agreed definition of digital trade; however, it is a term increasingly used to describe an ecosystem that is more expansive than "e-commerce," which is focused on trade in goods and services purchased online.[1] Digital trade includes the important role of cross-border data flows, and how data and digital technologies such as cloud computing and Artificial Intelligence (AI) can enable trade. The Organisation for Economic Co-operation and Development (OECD) defines digital trade as digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered and involve consumers, firms, and govern-

[1] WTO Work Programme on E-Commerce, 1998 definition of e-commerce is "the production, distribution, marketing, sale, or delivery of goods and services by electronic means."

ments.[2] Underpinning digital trade is the movement of data. Data is not only a means of production, but also an asset that can itself be traded, and a means through which global value chains are organized and services delivered. Furthermore, it indirectly supports physical trade by enabling implementation of trade facilitation.

The increasing scope of digital trade is reflected in various free trade agreements that now have digital trade chapters in place of e-commerce chapters.[3] These digital trade chapters include new commitments such as not to prohibit cross-border data flows and require data localization as a condition for doping business, subject to GATS Article XIV style exceptions.[4] Another trade policy development is the shift to digital economy agreements (DEAs), such as the U.S.-Japan Digital Trade Agreement or the Australia-Singapore Digital Economy Agreement.[5] These are digital-only agreements that often do not include new market access and instead focus on developing the rules and norms that can support digital trade. This includes regulation that builds trust in data flows and facilitates e-commerce.

OPPORTUNITIES FROM DIGITAL TRADE

Digital trade commitments, whether in FTAs or DEAs, can deliver potentially significant economic gains. The most recent assessment of the economic impacts of digital trade commitments was the U.S. ITC assessment of the economic impacts of USMCA that was published in April 2019.[6] According to the ITC assessment, a key driver of the economic gains for the U.S. from the USMCA come from its digital trade chapter. These rules were found to have a significant, positive impact on industries that rely on cross-border data flows, including for firms in the services economy, manufacturing, and agricultural industries, all of which rely on data and information flows in their business models, supply chains, and for international trade.

The following outlines the key elements of digital trade on how cross-border data flows enable e-commerce, services, and manufacturing exports, and can strengthen global value chains.

E-COMMERCE AND OPPORTUNITIES FOR SMALL AND MEDIUM-SIZED ENTERPRISES

There has been a lot of attention on the opportunities for SMEs of doing their business online, and therefore reaching customers globally. This was an early promise of the Internet in the 1990s and early 2000s that was not fully realized. While a lot of companies did build websites, this did not necessarily translate into sales in other countries. There were several reasons for this outcome, including payment systems that were costly and often could not support some of the elements required for cross-border e-commerce, such as processing returns. There was a lack of trust among consumers purchasing goods from businesses in third countries with limited recourse if the goods failed to arrive or were defective or damaged. It was also difficult to deliver the product in a timely and cost-effective way due to costly delivery services and inefficient Customs processes.

This has now changed. E-commerce presents a real opportunity for SMEs to export and reach customers globally, allowing small businesses to thrive and scale. A key development has been platforms such as eBay, Amazon, Etsy, Mercado Libre in South America, and Lazada in Asia. These platforms solve many of the previously mentioned problems. They provide integrated payment solutions, trust mechanisms, cheap and effective dispute settlement procedures, and links to express delivery services. Figure 1 compares SMEs on eBay that export compared to their offline peers. As can be seen, in the U.S. for example, 97 percent of small businesses on eBay export.

---

[2] *https://www.oecd.org/trade/topics/digital-trade/*.

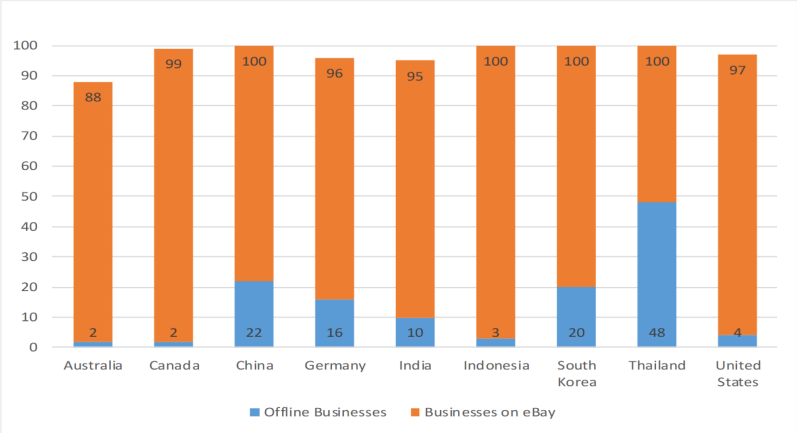
[3] For example, the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) and United States-Mexico-Canada Agreement (2019) include digital trade chapters whereas the U.S.-Australia FTA (2005) and U.S.-Singapore FTA (2004) have e-commerce chapters.

[4] *See for example* USMCA Article 19.11 and Article 19.12.

[5] Agreement between the United States of America and Japan Concerning Digital Trade.

[6] United States International Trade Commission. "U.S.-Mexico-Canada Trade Agreement: Likely Impact on the U.S. Economy and on Specific industry Sectors," April 2019, *https://www.usitc.gov/publications/332/pub4889.pdf*.

Figure 1: Small businesses almost always export on ebay



Source: eBay Small Online Business Growth Report 2016

The opportunities for SMEs to engage in digital trade has been enabled by various trade commitments. For instance, the WTO Trade Facilitation Agreement has helped reduce the costs of getting goods through Customs in many markets globally. In trade agreements such as the USMCA, commitments to raise the *de minimus* levels for Customs duties support the economic viability of smaller value transactions, often a staple of SME sales. Commitments on electronic signatures and electronic authentication provide important legal frameworks that allow for digital cross-border transactions. Commitments to not restrict data flows and to encourage interoperability among digital payment systems also enable the platforms that SMEs rely on to be global.

Another element that supports SMEs is access to digital technologies such as cloud computing. In fact, the cloud is an important enabler of a range of key inputs for all businesses. This includes leading edge software and computing capacity that is secure and available anywhere with an Internet connection. Cloud also supports businesses that provide access to attorneys, marketers, design professionals, and financial advisors on an at-need basis, supporting flexible and cost-effective solutions for small businesses.

THE U.S. LEADS THE WORLD IN DIGITAL SERVICE TRADE

The discussion around digital services leads to the broader observation that digital trade and cross-border data flows enable digital services exports. Before turning to digital services, it is worth noting the importance of services as a component of U.S. trade.

According to the U.S. Census Bureau, the U.S. services trade surplus (September 2021–September 2022) was $236.6 billion. This is a familiar and long-term trend—the U.S. has been exporting more services than it imports for over 30 years. Services now comprise around 40 percent of total U.S. trade.

But services are an even more significant part of overall U.S. trade than this share of services exports would suggest. This is because around 30 percent of U.S. goods exports comprise value-added services used in the production of goods. The net result is that over 60 percent of total U.S. exports comprise services.

The World Trade Organization (WTO) identifies four ways or modes that services can be exported:

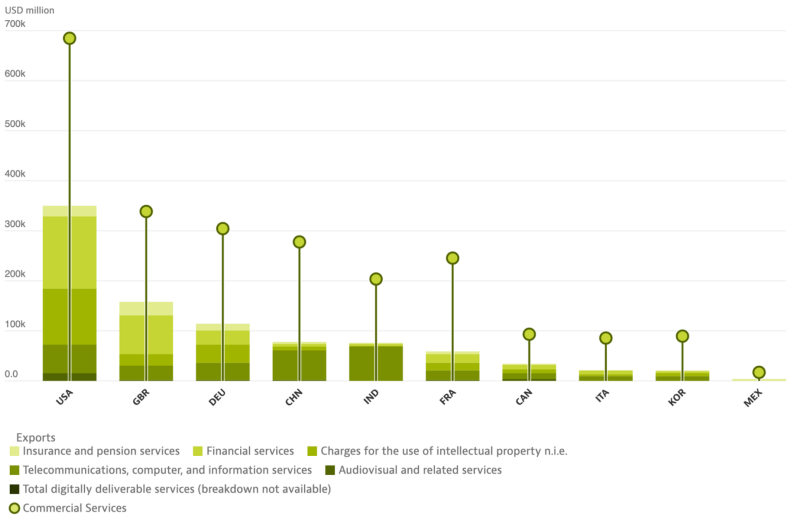
1. *Mode 1:* In a cross-border manner—where the service supplier does not leave the U.S. and provides the service online. This is a key vehicle for digital or online services trade.
2. *Mode 2:* When someone comes to the U.S. to consume a service such as tourists or students.

3. *Mode 3:* Where a U.S. business sets up a subsidiary overseas to provide a service, such as when Citibank opens a branch in Germany and provides financial services through that branch. Though in this example, much of this communication between the U.S. and the German branch will be online data will flow to enable communication, transfers for banking, and which allow the company to operate, such as information for human resources.
4. *Mode 4:* Services are traded internationally when people work in another country, a relatively small component of how services are exported.

These examples underscore that a lot of services can be exported and provided online. The following graph shows digitally deliverable services as a share of commercial services trade. Commercial services are key business inputs and comprise insurance and pension services, financial services, charges for the use of intellectual property, telecommunications, computer, and information services, and audiovisual and related services. Many of these services would be familiar to the average American consumer or small business owner. For example, PayPal is a digital financial service that enables cross-border e-commerce transactions on eBay, but also supports many e-commerce sites. Charges to IP can range from software licensing fees paid by a business to the commissions paid for artworks on Etsy. Small business owners may subscribe to Apple's iCloud in order to streamline the storage and security of data, as well as facilitate collaboration across platforms, such as Microsoft Teams. Digital native companies such as Allbirds or Bombas build their businesses almost exclusively using online advertising and social media networks to reach potential customers globally.

As can be seen in Figure 2, the U.S. is the world's largest exporter of digitally deliverable services, over three times larger than its nearest competitor Germany and 2.2 times larger than the UK. Moreover, 51 percent of U.S. exports of commercial services are digitally deliverable.

Figure 2: Digitally-deliverable exports of commercial services

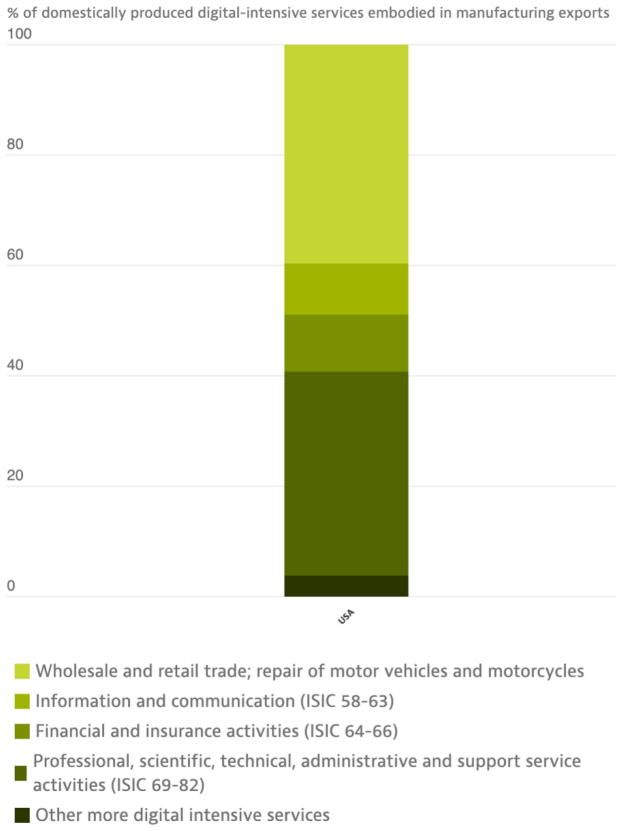


Source OECD (2020), https://goingdigital.oecd.org/indicator/71

DIGITALLY DELIVERABLE SERVICES ARE ALSO IMPORTANT FOR MANUFACTURING COMPETITIVENESS

As outlined, services comprise approximately 30 percent of U.S. manufactured exports, and many of these are digital services. The table below shows the percentages of domestically produced digital intensive services embodied in manufactured exports.

Figure 3: Digitally-intensive services value embodied in manufacturing exports



Source: OECD (2018) (https://goingdigital.oecd.org/indicator/70)

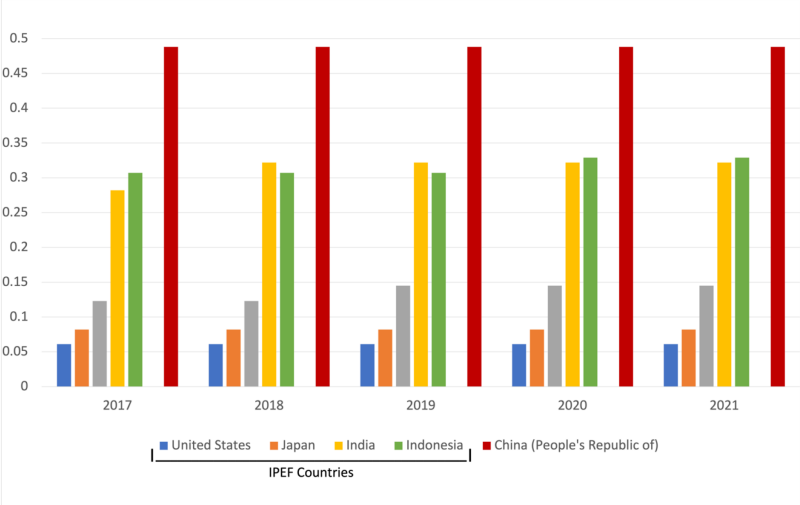
As can be seen, digital services used in manufacturing comprise professional, scientific, administrative, financial, ICT, and wholesale retail trade. For example, steel production is increasingly digitally intensive, relying on smart plants that knit together the manufacturing processes digitally to increase efficiency, and use AI systems that monitor and make adjustments to maximize performance. These types of uses of data and digital services play out across manufacturing—in automobiles, aircraft, medical products, and so on.

GROWING RESTRICTIONS ON DIGITAL TRADE

The digital trade opportunities for U.S. exporters increasingly face a global environment with high restrictions on digital trade. The OECD digital trade restrictiveness index shows relatively low levels of restrictions in the U.S. and relatively high levels of restrictions in Japan, India, and Indonesia—a set of countries participating in the Indo-Pacific Economic Framework (IPEF) negotiations. These restrictions also pale in comparison to China, which has one of the world's most restrictive digital trade regimes. They range from various personal data protection, cybersecurity, and national security laws that prohibit or severely restrict cross-border transfers of information. These laws often impose local data storage and processing requirements on companies that collect "important data," a broad and vaguely defined term. Many countries prevent U.S. companies from directly providing cloud computing services, including computer data processing and storage services and software application

services provided over the Internet. Many digital trade restrictions are also hurdles to electronic and Internet-enabled payment services such as slow licensing processes and data localization requirements.

Figure 4: OECD digital services trade restrictiveness index



DIGITAL TRADE AND ARTIFICIAL INTELLIGENCE

Digital trade also affects access to and the development of key digital technologies such as AI. Indeed, U.S. National Security Advisor Jake Sullivan has identified three families of technologies: (1) computing-related technologies that includes AI; (2) clean energy technologies; and (3) biotechnologies, all of which will affect U.S. security.[7] While the U.S. is a world leader in AI, many countries are moving to regulate AI and expand AI R&D in ways important for ongoing U.S. leadership in AI, and to which digital trade agreements can respond. This includes AI regulation that can restrict AI development and use. For instance, the European Union's AI Act that is moving through the EU Parliament will regulate high risk AI. In addition, Canada recently tabled its Artificial Intelligence and Data Act (AIDA). Meanwhile, China, which holds a unique position in the international AI landscape as both a chief collaborator with the U.S. on AI R&D and competitor, has begun to roll out its own AI governance framework. This includes regulations on the development and deployment of AI algorithms, as well as increased control over Chinese technology firms leading in AI development. China is also exporting its model for AI regulation to other countries in the Indo-Pacific and globally.

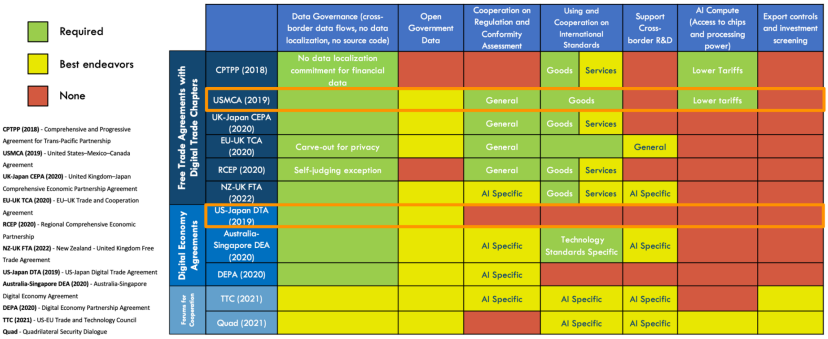
Some countries are using FTAs and DEA to support AI specifically, but the U.S. has yet to do so. Relevant ways that digital trade commitments can support AI regulation and R&D include around access to data, agreements on using technology standards developed in multistakeholder standards setting bodies, agreement that AI regulation should be risk-based, and support for collaboration on AI R&D among like-minded countries.

The following table was developed in the Forum on Cooperation in AI (FCAI), which I co-lead with Cameron Kerry and Andrea Renda. FCAI is a track 1.5 dialogue among seven governments, industry, and civil society that aims to identify areas for international collaboration in AI.[8]

[7] Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit, The White House, *https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/*.

[8] The Forum for Cooperation on Artificial Intelligence, *https://www.brookings.edu/project/the-forum-for-cooperation-on-artificial-intelligence/*.

Figure 5: Digital trade commitments can support AI



This table shows the ways that trade agreements can support AI. While the USMCA and the U.S.-Japan Digital Trade Agreement include relevant commitments, none of these are AI specific. In contrast, other countries have taken the next step and began articulating AI specific commitments. For example, the Australia-Singapore Digital Economy Agreement, the EU-UK Trade and Cooperation Agreement, and the New Zealand-UK Free Trade Agreement include AI-specific commitments. While the U.S. does continue to focus on AI in other spaces, such as the TTC and the Quad, digital trade commitments present an important opportunity to influence AI regulatory developments, ensure markets are open and competitive, and support AI R&D among allies and partner countries.

CONCLUSION

The U.S. has been perhaps most effective at developing a world class digital economy that has created a range of new opportunities for digital trade for both small and large businesses. However, to date the U.S. has not sufficiently engaged nor shaped the rules and norms for how digital trade should assess risks that impact access to new markets. The U.S. should therefore work in cooperation with many governments that are working hard to regulate and develop their own digital economies and shape the terms of digital trade. And most importantly, U.S. leadership in developing rules that govern digital technologies such as AI is needed to ensure that AI is appropriately regulated and developed consistently with U.S. values. The forthcoming IPEF negotiations is the next opportunity for the U.S. to craft the next generation of digital trade rules that can support a range of economic opportunities that digital trade provides.

PREPARED STATEMENT OF PATRICK WOODALL, POLICY AND RESEARCH DIRECTOR, AFL–CIO TECHNOLOGY INSTITUTE

Thank you, Chairman Carper and Ranking Member Cornyn, for the opportunity to testify before your committee on "Opportunities and Challenges for Trade Policy in the Digital Economy." This testimony is submitted on behalf of the AFL–CIO Technology Institute and the American Federation of Labor and Congress of Industrial Organizations and the 12.5 million workers represented by its 58 affiliated unions.

The digital transformation of the economy has generated real societal gains—with significant scientific, communications, health-care, commercial, and other advances—but also raised urgent challenges for workers and society. This rapid technological change 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 digital revolution. The U.S. Congress and U.S. regulators as well as governments worldwide are only beginning to confront these challenges.

Digital commerce and cross-border digital trade affects people at work and at home as technologies become built into workplaces and daily life. Digital commerce and digital trade covers any services or products that are delivered over the Inter-

net. Much of this is consumer-facing content or services like e-books and movies, email services, smartphone apps, and software downloads. But it also concerns the backbone of e-commerce (everything except the delivery of goods purchased online), global cloud computing, and the big data services that undergird an increasing portion of big business operations and impact workers on and off the job.

The forces of global digital commerce are dramatically affecting millions of workers whether they know it or not. These workers include back-office and call-center workers that can lose their jobs from digital offshoring to countries where workers are paid poverty wages and face severe repression for organizing trade unions. They include workers whose jobs are managed or controlled by automated software that hires, rates, fires, schedules, and prods them to work faster to hit ramped-up productivity targets. These technologies can shortchange workers' earnings, expose workers to unsafe workplace conditions, infringe on the right to form unions, and exacerbate employment discrimination. Digital trade includes low-paid workers who toil for platform companies that assign tasks, set pay rates, and impose unaccountable discipline on "gig" workers who endure low earnings, uncertain work schedules, and no benefits. And workers everywhere who are monitored on and off the job by their employers.

Working families face the threats of digitization outside the workplace as well. 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.

The digital trade rules set the parameters of how governments can address these global data flows and cross-border software that affects workers, consumers, and society. The current digital trade rules, included in the U.S.-Mexico-Canada Agreement and the U.S.-Japan digital trade agreement, grant broad powers to the companies that control these technologies and data and set stringent prohibitions against government efforts to curb the demonstrable excesses of the digital economy.

There needs to be a new way forward for digital trade that prioritizes workers and people and not just the technology industry. 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] This requires 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.

A new worker-centered approach to digital trade 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. The absence of domestic measures governing the digital economy heightens the importance that digital trade agreements must preserve robust public policy space.

This testimony describes the significant problems with granting broad powers to cross-border digital trade while narrowly constraining government oversight in the context of trade approaches of other sectors (Section I). It discusses the issues around digital trade provisions on cross-border data flows and data localization (Section II), source codes and algorithms (Section III), and other digital trade issues that impact workers and society (Section III).

I. EXISTING DIGITAL TRADE RIGID CONSTRAINTS ON DOMESTIC GOVERNANCE ARE INAPPROPRIATE BECAUSE DIGITAL IS DIFFERENT

The past 3 decades of globalization and international trade have cost millions of American manufacturing and service-sector jobs and contributed to the widening economic and racial inequality in the United States. Prior trade agreements focused on the shipments of physical goods and cross-border services but also addressed so-called regulatory non-tariff barriers to trade that affected goods and services. These trade provisions were adopted long after industrialized countries had established

[1] Tai, Katherine. (Ambassador Tai). 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 *(https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2021/november/remarks-ambassador-katherine-tai-digital-trade-georgetown-university-law-center-virtual-conference).*

regulatory structures designed to protect workers, consumers, the environment, and communities from unsafe workplaces, dangerous products, and pollution.

But the current provisions in digital trade are fundamentally different. First, they grant broader powers to the technology companies and employers that deploy digital technologies and ship data worldwide than have previously been included in trade provisions. Second, the digital trade language sets far narrower constraints on government oversight of these cross-border data and technology transactions and transmissions than in other sectors. The combination of these two elements delivers a far more unbalanced combination of unilateral corporate power for big tech with far more rigid constraints on domestic oversight of the ubiquitous technologies and data that govern workers' lives at home and on the job.

Critically, existing U.S. digital trade provisions are delivering these broad cross-border corporate powers unfettered by government regulation when the United States and many trading partners have almost no regulatory structures to address the excesses of the technology industry. The United States has only a patchwork of laws and rules that govern big tech business models and expanding the current digital trade model would effectively lock in an unregulated technology sector with little or no meaningful oversight. The technology companies have pushed for tough digital provisions to "lock in their political power in international rules that are difficult to change," according to a 2016 London School of Economics paper.[2] Providing meaningful public policy space that is not curtailed by digital trade provisions is especially crucial for the new and novel concerns that are rapidly impacting workers and society.

Trade agreements infringe on domestic governance: Trade agreements were designed to reduce barriers to cross-border shipments of goods, largely import tariffs and quotas but increasingly domestic regulations that are deemed so-called non-tariff barriers. Over the past 3 decades, tariffs were substantially reduced or eliminated through multilateral or bilateral trade agreements. In the United States, this led to a dramatic surge in imports that cost millions of U.S. manufacturing jobs and created far more vulnerable supply chains.[3] Unlike physical goods, there has been a tariff moratorium on cross-border data flows, electronic transmissions, and e-commerce transactions since 1998.[4]

The trade agreements since the 1990s have also aimed to curb domestic regulations that purportedly act as non-tariff barriers to cross-border trade. The World Trade Organization and other bilateral agreements constrained domestic governance over workplace safety, the environment, food safety, regulatory standards and more. These agreements imposed significant limitations on governments' ability to implement policies that can affect trade and brought domestic governance under the disciplines of trade dispute settlement.

Trading partners can demand that domestic policies (or measures, in trade language) be assessed to determine whether they pose illegitimate trade barriers. These evaluations are significantly biased against the ability of governments to establish domestic policies to protect workers, consumers, communities, or the environment. Policies are evaluated on a series of trade tests (the legitimacy and necessity of the measure, the trade restrictiveness or whether a less protective measure would facilitate more trade, and whether the measure poses arbitrary or unjustified non-discrimination, including whether it is a disguised trade restriction).

These policy caveats have proven difficult for countries to invoke in practice, even for sectors with longstanding, well-established regulatory regimes. At the World Trade Organization (WTO), fewer than 5 percent of domestic measures that were

---

[2] Azmeh, Shamel and Christopher Foster. London School of Economics. "The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements." Working Paper No. 16-175. January 2016 at 7 *(https://www.semanticscholar.org/paper/The-TPP-and-the-digital-trade-agenda%3A-Digital-and-Azmeh-Foster/bead20d05f43cbbde351a4cc42f2112773ff1039).*

[3] Scott, Robert E. and Zane Mokhiber. Economic Policy Institute. "Growing China trade deficit cost 3.7 million American jobs between 2001 and 2018." January 30, 2020 *(https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/);* Acemoglu, Daron et al. National Bureau of Economic Research. "Import Competition and the Great U.S. Employment Sag of the 2000s." Working Paper No. 20395. August 2014 *(https://www.nber.org/papers/w20395).*

[4] Farge, Emma. "WTO provisionally agrees to extend e-commerce tariff moratorium—sources." Reuters. June 16, 2022 *(https://www.reuters.com/markets/commodities/wto-provisionally-agrees-extend-e-commerce-tariff-moratorium-sources-2022-06-16/).*

challenged as illegal trade barriers were upheld in trade disputes as trade-legal under these regulatory exceptions.[5]

The prior trade agreements' approach to domestic regulations over goods and services were built upon an architecture of longstanding domestic regulatory regimes in countries like the United States. Even the severe bias against domestic regulations often contained language that affirmatively granted the right to regulate and established guidelines for evaluating domestic regulations to purportedly ensure they were consistent with the international commitments.[6] These approaches at least recognized that global trade commitments interacted with robust domestic regulatory policies.

Digital trade provisions include tough proscriptions against domestic governance: The existing digital trade provisions grant more powerful constraints on domestic policymaking in an environment where there is little or no regulatory oversight of the technology sector. The technology industry generally views all efforts to regulate digital commerce and trade—including in areas like privacy protection and national security—as illegitimate trade barriers motivated more by parochial protectionism than by legitimate public policy concerns.[7]

Many USMCA and the U.S.-Japan digital provisions include prohibitions against domestic regulations. For example, the agreements dictate that "no party shall prohibit or restrict" cross-border data flows,[8] "no party shall require" local data storage,[9] "no party shall require" access to software source codes,[10] and "no party shall adopt or maintain" policies that hold platforms accountable for the content posted on their networks.[11]

This digital language begins with broad prohibitions against domestic governance which sets a presumption that any domestic laws or regulations to safeguard workers or consumers from the excesses of the technology industry could be deemed illegal trade barriers. Some provisions contain the same weak trade policy caveats (legitimate, necessary, minimally trade restrictive, and disguised protectionism) that make it harder to establish domestic policies to protect workers and consumers from the downsides of digitization.[12]

The significant constraints on domestic governance could make it easier for trading partners to challenge any future regulatory efforts to rein in the technology industry and protect workers and consumers. This effectively would lock in the current absence of regulatory oversight of big tech in the United States.[13]

Constraint of governance over unregulated technology: The United States has a patchwork of largely outdated statutes and regulations that fail to protect people and workers from the potential abuses of the digital world. Federal laws protecting personal data cover some specific areas (like medical information, credit, or financial data), but do not require companies to notify or compensate people if their personal information is shared or sold or exposed to unauthorized parties through cyber-

---

[5] Rangel, Daniel. Public Citizen's Global Trade Watch. "WTO General Exceptions: Trade Law's Faulty Ivory Tower." January 2022 *(https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/).*

[6] For example, the WTO Sanitary and Phytosanitary Agreement Art. 2.1 gave members "the right to take sanitary and phytosanitary measures necessary for the protection of human, animal or plant life or health, provided that such measures are not inconsistent with the provisions of this Agreement.

[7] Horowitz, Jeff. "U.S. International Trade Commission's Digital Trade Roundtable: Discussion Summary." *Journal of International Commerce and Economics.* October 2015 at 3 *(https://www.usitc.gov/publications/332/journals/vol_iv_article4_digital_trade_summary.pdf).*

[8] U.S.-Mexico-Canada Agreement (USMCA) Art. 19.11.1 *(https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf);* U.S.-Japan Digital Trade Agreement (U.S.-Japan). Art. 14.11.1 *(https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf).*

[9] USMCA Art. 19.12; U.S.-Japan Art. 12.

[10] USMCA Art. 19.16.1; U.S.-Japan Art. 17.1.

[11] USMCA Art. 19.17.2; U.S.-Japan Art. 18.2.

[12] USMCA Art. 19.11.1 and U.S.-Japan Art. 11.1.

[13] Azmeh, Shamel, Christopher Foster, and Jaime Echavarri. (Azmeh, Foster and Echavarri). "The International Trade Regime and the Quest for Free Digital Trade." *International Studies Review.* Vol. 22. 2020 at 684 *(https://academic.oup.com/isr/article/22/3/671/5564378).*

crime or data breaches.[14] Many of the laws are outdated for today's digital world.[15] For example, the rules that absolve platforms and social media companies from responsibility from users promoting hate speech and disinformation were implemented during the age of dial-up modems.[16]

There are effectively no regulations overseeing the impact of algorithmic management, and workers have little protection or recourse from digital surveillance on or even off the job.[17] Automated recruiting, hiring, and promotional decisions can have disproportionate or disparate impact on people of color, women, people with disabilities, older people, immigrants, or other protected classes, but the application of civil rights statutes to new and emerging digital technologies remains murky.[18]

The public and the Congress recognize that this big tech Wild West is not working for people or society. An increasing majority of the public favors more regulation of technology and technology companies, especially related to protecting privacy and curbing monopolistic market power.[19] The House Energy and Commerce Committee passed digital privacy legislation nearly unanimously in July 2022 and released a bipartisan statement flagging the legislation's goal to "rein in big tech's power and establish clear, robust protections for people."[20] Bipartisan legislation to address big tech's monopolistic and anticompetitive power has passed the Senate and House Judiciary committees but has faced a withering and misleading advertising campaign to derail the legislation.[21] The existing digital trade language would create a very high barrier to implementing and enforcing these laudable congressional efforts.

The existing digital trade provisions constraints on domestic governance harm workers, consumers, and society. The following sections describe how the combination of broad corporate powers for big tech companies and stringent regulatory restrictions could lead to increased offshoring of U.S. jobs, make it harder to enforce current labor, employment, and civil rights laws against artificial intelligence algorithmic management and automated decision-making, and prevent governments from adopting safeguards to address emerging technological issues, such as workplace surveillance.

II. WORKERS HARMED BY FREE FLOW OF DATA AND DATA LOCALIZATION DIGITAL TRADE PROVISIONS THAT ACCELERATE JOB OFFSHORING AND PREVENT PROTECTING CRITICAL DATA AND SECTORS

The current digital trade model grants broad powers to technology and other companies to control, transmit, process, and store data worldwide, while also shielding their digital systems from regulatory scrutiny. These provisions prohibit any restric-

---

[14] Klosowski, Thorin. "The state of consumer data and privacy laws in the US (and why it matters)." *New York Times.* September 6, 2021 *(https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/).*

[15] Kerry, Cameron F. Brookings Institute. "Why protecting privacy is a losing game today—and how to change the game." July 12, 2018 *(https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/).*

[16] The Digital Millennium Copyright Act of 1998. 17 U.S.C. § 512.

[17] Bernhardt, Annette, Lisa Kresge, and Reese Suliman. (Bernhard, Kresge and Suliman). University of California Berkeley Labor Center. "Data and Algorithms at Work: The Case for Worker Technology Rights." November 2021 at 2 *(https://laborcenter.berkeley.edu/data-algorithms-at-work/);* Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. (Ajunwa, Crawford, and Schultz). "Limitless Worker Surveillance." *California Law Review.* Vol. 105. 2017 at 747 to 749 *(https://californialawreview.org/print/3-limitless-worker-surveillance/).*

[18] Yang, Jenny R. Urban Institute. (Yang). Statement before the Subcommittee on Civil Rights and Human Services. Committee on Education and Labor. U.S. House of Representatives. "The Future of Work: Protecting Workers' Civil Rights in the Digital Age." February 5, 2020 at 8 to 11 *(https://edworkforce.house.gov/download/jenny-r-yang/default.aspx).*

[19] Vogels, Emily A. Pew Research Center. "56% of Americans support more regulation of major technology companies." July 20, 2021 *(https://www.pewresearch.org/fact-tank/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/);* Brenan, Megan. Gallup. "Views of Big Tech Worsen; Public Wants More Regulation." February 18, 2021 *(https://news.gallup.com/poll/329666/views-big-tech-worsen-public-wants-regulation.aspx).*

[20] U.S. House of Representatives. Energy and Commerce Committee. [Press release]. "Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act." July 20, 2022 *(https://republicans-energycommerce.house.gov/news/press-release/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy-and-protection-act).*

[21] Feiner, Lauren. "Senate committee votes to advance major tech antitrust bill." CNBC. January 20, 2022 *(https://www.cnbc.com/2022/01/20/senate-committee-votes-to-advance-major-tech-antitrust-bill.html);* McKinnon, John D. "Big Tech Has Spent $36 million on Ads to Torpedo Antitrust Bill." *Wall Street Journal.* June 9, 2022; Wheeler, Tom. Brookings Institute. "History repeats itself with Big Tech's misleading advertising." June 15, 2022 *(https://www.brookings.edu/blog/techtank/2022/06/15/history-repeats-itself-with-big-techs-misleading-advertising/).*

tion on cross-border data flows—even for sensitive forms of personal information—as well as an absolute prohibition on "data localization" policies. Together, these two provisions grant companies a near unrestricted right to control data and ship it worldwide. The globalization of data has led to the outsourcing and offshoring of U.S. jobs, the increasing privatization of government datasets that reduces public access and raises costs, and the collection of vast troves of personal data compromises the privacy of workers on the job and people at home.

Tech industry demands and existing digital provisions deliver unfettered free flow of data: The technology industry and other big businesses have pressed for digital trade provisions that largely prohibit any impediments to cross-border data flows. The U.S. technology industry has pressed hard for free flow of data because the biggest cloud computing firms are based in the United States.[22] The U.S. Chamber of Commerce listed unfettered cross-border data flows as its top digital trade priority.[23] The industry promotes the unrestricted right for companies to transfer data across borders as a tool to counter authoritarian Internet censorship,[24] but that does not mean that all data—including personal, sensitive, or secure—should have no restrictions or requirements when crossing borders.[25]

These industry demands are enshrined in existing digital trade language that provide a nearly unrestricted, unconditional right for cross-border data collection, transmission, and use. The USMCA and U.S. Japan digital agreement both contain nearly absolutist language on data flows: "No Party shall prohibit or restrict the cross-border transfer of information" and it specifically includes "personal information" in this protected right to ship data worldwide.[26] This prioritizes corporate data ownership and control over the privacy rights of workers and consumers.

The USMCA and the U.S.-Japan cross-border data flow provisions contain only narrow caveats for permissible government measures that must be necessary, legitimate, not disguised restriction to trade, or more trade restrictive than necessary.[27] These policy exceptions are borrowed from the WTO, where dispute panels have narrowly interpreted these caveats and constrained governments' right to regulate. The current digital provisions would make it very difficult for governments to maintain or adopt rigorous measures to address the negative impacts of unrestricted data flows on workers or consumers.

Prohibitions on data localization can harm workers, consumers, and the economy: The USMCA and U.S.-Japan digital provisions also contain an absolute prohibition on "data localization" policies. Data localization measures require that data generated within a country must meet certain requirements including domestic data storage.[28] An increasing number of governments are requiring that some kinds of data be stored on domestically to protect digital privacy or secure critical infrastructure.

The USMCA and U.S.-Japan data localization provisions broadly prohibit countries from requiring companies "to use or locate computing facilities in that party's territory as a condition for conducting business."[29] Unlike the prohibition on restrictions to cross-border data flows, neither digital agreement contains a "legitimate public policy" exception, although both agreements exclude financial services from the data localization provisions.[30]

While some data localization policies have been established to foster domestic capacity or protect domestic industries, many "localization policies may be used to achieve legitimate public policy objective, including national security and personal

---

[22] Fefer, Rachel F., Shayerah I. Akhtar, and Michael D. Sutherland. (Fefer, Akhtar and Sutherland). Congressional Research Service. "Digital Trade and U.S. Trade Policy." CRS Report R44565. December 9, 2021 at 17 *(https://crsreports.congress.gov/product/pdf/R/R44565/18).*

[23] U.S. Chamber of Commerce. "The Digital Trade Revolution: How U.S. Workers and Companies Can Benefit from a Digital Trade Agreement." February 2022 at 18 *(https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022.pdf).*

[24] Cory, Nigel, Robert D. Atkinson, and Daniel Castro. Information Technology and Innovation Foundation. "Principles and Policies for 'Data Free Flow with Trust.'" May 27, 2019 *(https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust/).*

[25] McCann, Duncan. (McCann). New Economics Foundation. For the International Trade Union Confederation. "Free Trade Agreements, Digital Chapters and the impact on Labor." 2019 at 16 *(https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf).*

[26] USMCA Art. 19.11.1 and U.S.-Japan Art. 11.1.

[27] USMCA Art. 19.11.2 and U.S.-Japan Art. 11.2.

[28] Azmeh, Foster and Echavarri. 2020 at 677 *(https://academic.oup.com/isr/article/22/3/671/5564378).*

[29] USMCA Art. 19.12; U.S.-Japan Art. 12.1.

[30] USMCA Art. 19.1; U.S.-Japan Art. 12.2.

data protection," according to the Congressional Research Service.[31] Localization requirements can also prevent companies from moving data to countries with the weakest privacy or financial protections in a digital race to the bottom that could shield information from regulatory oversight.[32]

The combination of the unfettered right to ship data across borders and prohibitions against maintaining domestic data storage to secure some categories of sensitive data or some critical economic sectors can harm consumers, workers, and the economy. For example:

- *Digital trade provisions compromise personal privacy:* 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. Privacy issues are inherently tangled with digital trade issues by companies that collect and ship personal data across borders.[33] Tech companies view privacy measures that keep critical data either within national borders or subject to stronger oversight requirements as "impediments to the presence and productivity of their companies in these countries and to international trade," according to companies at a U.S. International Trade Commission forum.[34] The Office of the U.S. Trade Representative (USTR) has identified consumer privacy measures as potential or likely trade barriers and unreasonable impediments to the cross-border flow of data, including laws in Canada, EU, India, Israel, Korea, and Switzerland.[35]

  The USMCA and U.S.-Japan digital provisions explicitly state that even the cross-border transmission of "personal information" cannot be prohibited or restricted.[36] The agreements purportedly permit policies to safeguard personal information but effectively encourage voluntary, corporate self-regulation as a substitute for government privacy regulations.[37] But voluntary, self-regulation is what consumers face today and it is not working. The big tech companies that own the personal data already have "privacy" policies but have nonetheless exposed users to cyber-risks while monetizing the data they collect.[38] The digital trade personal information provisions also require regulatory approaches be "necessary and proportionate to the risks,"[39] but do not recognize that consumers, not the companies, bear all the digital privacy risks. This prevents the enactment of any meaningful privacy protection, because it can be difficult to put a financial value on privacy and security from cyber-breaches.[40]

- *Current digital provisions contain no exceptions for critical infrastructure:* The USMCA and U.S.-Japan data provisions do not exclude critical infrastructure.[41] Failing to exempt critical infrastructure from the cross-border data

---

[31] Fefer, Akhtar and Sutherland. 2021 at 16 *(https://crsreports.congress.gov/product/pdf/R/R44565/18).*

[32] Kelsey, Jane. Public Services International. "Digital trade rules and Big Tech: Surrendering the public good to private power." February 2020 at 14 to 15 *(https://publicservices.international/resources/publications/digital-trade-rules-and-big-tech-surrendering-public-good-to-private-power?id=10825&lang=en).*

[33] Azmeh, Foster and Echavarri. 2020 at 682 *(https://academic.oup.com/isr/article/22/3/671/5564378).*

[34] Horowitz, Jeff. "U.S. International Trade Commission's Digital Trade Roundtable: Discussion Summary." *Journal of International Commerce and Economics.* October, 2015 at 4 *(https://www.usitc.gov/publications/332/journals/vol_iv_article4_digital_trade_summary.pdf).*

[35] Office of the U.S. Trade Representative (USTR). "2021 National Trade Estimate Report on Foreign Trade Barriers." March 2021 at 89, 209, 266, 289, 332 *(https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf).*

[36] USMCA Art. 19.11.1; U.S.-Japan Art. 11.2.

[37] USMCA Art. 19.8.2 footnote 4; U.S.-Japan Art. 15.1 footnote 12.

[38] Warzel, Charlie and Stuart A. Thompson. "Tech Companies Say They Care." *New York Times.* April 10, 2019 *(https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html).*

[39] USMCA Art. 19.8.3; U.S.-Japan Art. 15.4.

[40] Estevadeordal, Anton, Marisol Rodriguez Chatruc, and Christian Volpe Martincus. Inter-American Development Bank. "New Technologies and Trade: New Determinants, Modalities, and Varieties." Discussion Paper No. IDB-DP-00746. February 2020 at 25 *(https://publications.iadb.org/publications/english/document/New_Technologies_and_Trade_New_Determinants_Modalities_and_Varieties_en.pdf).*

[41] The Comprehensive and Progressive Agreement for Trans-Pacific Partnership, to which the United States is not a party, did exempt critical infrastructure from the agreement's software secrecy provisions. CPTTP Art. 14.17.2 *(https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf).*

and data localization provisions could make it harder to protect essential economic sectors from cyberattacks. In 2021, a cyberattack against one of the biggest pipeline systems on the east coast led to gas lines and threatened to idle downstream industry like chemical companies and refineries.[42] Another 2021 hack of a Florida water system remotely elevated the levels of a dangerous chemical in the water; the operator fortunately noticed the change and quickly prevented the hack from tainting the water supply.[43] The Government Accountability Office has highlighted the environmental and economic risks of the cyber vulnerability of 1,600 U.S. offshore oil and gas rigs.[44] Some companies and countries are moving towards domestic data hosting for critical infrastructure to increase security and accountability for systems like electricity and water delivery.[45]

- *Digital trade data provisions encourage low-road digital offshoring:* 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. According to a 2021 report commissioned by Facebook, "If transferring personal data were not permitted, offshoring business services to popular outsourcing destinations would no longer be possible."[46] This kind of digital outsourcing has eliminated U.S. jobs and cost workers their benefits.[47] One call center outsourcing company promotes a list of nearly 30 major corporations—including financial and telecommunications firms—that outsource their call centers.[48] AT&T shuttered 44 call centers costing 16,000 unionized Communications Workers of America (CWA) jobs from 2011 to 2018, despite record profits.[49] A 2018 Labor Department investigation found that Wells Fargo slashed thousands of U.S. customer service and technology jobs while hiring overseas workers to replace the exact same functions.[50]

Many of these jobs are going to countries where workers and union activists face severe repression and toil for low wages with few labor protections. For example, many of the CWA call center jobs have been digitally offshored to countries like Mexico and the Philippines.[51]

The digital trade data provisions also help maintain a global underclass of low-paid gig workers who transcribe, enter data, label images, and manually tag information that powers the artificial intelligence systems of the biggest tech compa-

---

[42] Sanger, David E. and Nicole Perlroth. "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity." *New York Times.* June 8, 2021 *(https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html).*

[43] Margolin, Josh and Ivan Pereira. "Outdated computer system exploited in Florida water treatment hack." ABC News. February 11, 2021 *(https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550).*

[44] Government Accountability Office. "Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure." GAO–23–105789. October 26, 2022 *(https://www.gao.gov/products/gao-23-105789).*

[45] "Mitigating risks through sovereign data services." CRN News. November 21, 2022 *(https://www.crn.com.au/feature/mitigating-risks-through-sovereign-data-services-588052).*

[46] Kepes, Roze, Josh White, and Aaron Yeater. Analysis Group for Facebook. "The importance of cross-border data flows." June 2021 at 4 *(https://about.fb.com/wp-content/uploads/2021/06/The-Importance-of-Cross-Border-Data-Flows.pdf).*

[47] Chakraborty, Kalyan and William Remington. "Impact of Offshore Outsourcing of IT Services on the U.S. Economy." *Southwestern Economic Review.* 2004 *(https://swer.wtamu.edu/sites/default/files/Data/73-94-69-258-1-PB.pdf).*

[48] Magellan Solutions. "List of Companies That Outsource Call Centers." Accessed March 2022 *(https://www.magellan-solutions.com/blog/list-of-companies-that-outsource-call-centers/).*

[49] Sainato, Michael. "'They're liquidating us': AT&T continues layoffs and outsourcing despite profits." *The Guardian.* August 18, 2018 *(https://www.theguardian.com/us-news/2018/aug/28/att-earns-record-profits-layoffs-outsourcing-continue);* Communication Workers of America (CWA). "AT&T 2018 Jobs Report." April 25, 2018 *(https://www.cwa-union.org/sites/default/files/att-jobs-report-2018.pdf).*

[50] Moise, Imani. "Wells Fargo moves jobs abroad after U.S. layoffs, government says." Reuters. December 20, 2018 *(https://www.reuters.com/article/us-wells-fargo-outsourcing/wells-fargo-moves-jobs-abroad-after-u-s-layoffs-government-says-idUSKCN1OJ2V5).*

[51] CWA. "Offshoring Security." October 2013 *(https://www.scribd.com/document/183863856/OFFSHORING-SECURITY-How-Overseas-Call-Centers-Threaten-U-S-Jobs-Consumer-Privacy-and-Data-Security#fullscreen=1);* CWA. [Press release]. "CWA Uncovers Massive Verizon Offshoring Operation in Philippines." May 13, 2016 *(https://cwa-union.org/news/releases/cwa-uncovers-massive-verizon-offshoring-operation-in-philippines).*

nies.[52] Many of these millions of ghost workers are in Indo-Pacific Economic Framework countries India and the Philippines where they receive low pay and precarious labor conditions.[53] Companies in the United States are the biggest employers of digital gig workers in the developing world according to data compiled by the University of Oxford.[54]

A worker-centered digital trade agenda would establish critical safeguards for workers, consumers, and the economy: Future digital trade agreements must provide robust public policy space to protect workers, consumers, and the economy. The current digital provisions excessively constrain domestic policy and do not provide necessary flexibility to address emerging and novel technological issues. At a minimum, the cross-border data and data localization provisions of future digital trade agreements or compacts should:

- *Authorize and encourage governments to enact 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 their citizens' personal data. 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 establish stronger requirements for data related to certain sensitive sectors or personal information, including critical infrastructure (energy, water systems, transportation), national security, law enforcement, health care, finance, and other areas where a data breach or disruption risks undermining economic or national security. 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.

III. WORKERS HARMED BY SOURCE CODE AND ALGORITHM DIGITAL TRADE PROVISIONS THAT SET HIGH BARRIERS TO ADDRESS CORROSIVE IMPACTS OF BOSS-WARE

Current U.S. digital trade agreements include broad prohibitions on government access to and oversight of the source codes and algorithms behind the automated decision-making and artificial intelligence systems that are increasingly impacting the workplace and society. The provisions purport to be focused on preventing the forced transfer of software secrets as a condition for market access, but the strong, binding source code and algorithm protections pose significant challenges for effective government oversight.[55]

Source code is the description of the steps or actions a computer program takes to perform its functions. Software source code is often "black box" technology that is not transparent to software consumers, meaning even the companies that buy and deploy these programs do not know how they work. These source codes and algorithms are also the recipe for how companies extract and commodify personal data and increasingly govern the workplace and oversee workers.

There are many legitimate policy reasons for government authorities to examine source codes and algorithms. For example, financial regulators might want to access source codes and trading algorithms to prevent high-frequency securities trading from engaging in market manipulation.[56] Environmental regulators should be able

---

[52] Friedland, Julian, David Balkin, and Ramiro Montealegre. "A Ghost Workers' Bill of Rights: How to Establish a Fair and Safe Gig Work Platform." California Management Review. January 7, 2020 *(https://cmr.berkeley.edu/2020/01/ghost-workers/).*

[53] Royer, Alexandrine. Brookings Institute. "The urgent need for regulating global ghost work." February 9, 2021 *(https://www.brookings.edu/techstream/the-urgent-need-for-regulating-global-ghost-work/).*

[54] Kässi, Otto and Vili Lehdonvirta. Oxford Internet Institute. University of Oxford. "Online Labour Index 2020 by Country." 2020 *(http://onlinelabourobservatory.org/oli-demand/).*

[55] Slok-Wódkowska, Magdalena and Joanna Mazur. (Slok-Wódkowska and Mazur). "Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code." *Journal of International Economic Law*. Vol. 25. 2022 at 107 *(https://academic.oup.com/jiel/article/25/1/91/6534278).*

[56] Busch, Danny. "MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct market access." *Law and Financial Markets Review.* Vol. 10, Iss. 2. 2016 *(https://www.tandfonline.com/doi/full/10.1080/17521440.2016.1200333).*

to determine if pollution-evasion software facilitates increased emissions, as was the case with the Volkswagen diesel emissions fraud.[57]

Ambassador Katherine Tai stated that digital trade provisions need to provide policy space to address "artificial intelligence in a way that safeguards economic security for workers."[58] But the current digital trade provisions create substantial barriers to governments accessing source code and algorithms to protect workers and enforce labor laws, protect privacy, enforce civil rights laws and prohibit discrimination, safeguard consumers, police anticompetitive conduct, and to pursue other legitimate public policy goals.

Digital trade source code and algorithm secrecy provisions constrain legitimate government oversight: The USMCA and U.S.-Japan source code provisions impose broad prohibitions on necessary government oversight and lock in the current weak regulatory oversight of algorithmic management in the workplace leaving workers and people unprotected from the excesses of digitization. These agreements prohibit countries from requiring "the transfer of, or access to, a source code of software [. . .] or an algorithm expressed in that source code" as a condition of distributing or selling that product.[59] The USMCA definition of algorithm (a "defined sequence of steps taken to solve a problem or obtain a result"[60]) might preclude governments from accessing even a description of what data the source code uses, how the data is evaluated, and how the source code operates.[61] The source code provisions shield technology companies and employers from government efforts to monitor and access source codes and algorithms even to achieve needed policy goals to protect the public.

The existing digital agreements provide a narrow exception that allows government oversight "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding."[62] The case-by-case exemption for *specific* enforcement actions precludes broader, industry-wide evaluations of big tech to curb 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 artificial intelligence-driven 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.[63]

Digital source code and algorithm provisions could prevent the protection of workers from the excesses of algorithmic management: Employers are increasingly using artificial intelligence and other software automation applications to screen potential workers, assign tasks, press workers to be more productive, set shift schedules and pay rates, and discipline and terminate workers.[64] Women, people of color, and immigrants are more likely to be employed in lower-wage workplaces where they can bear the brunt of algorithmic management and its potentially embedded racial and social biases.[65] These trends increased during the pandemic shift to remote and hybrid work.[66]

---

[57] Dwyer, Jim. "Volkswagen's Diesel Fraud Makes Critic of Secret Code a Prophet." *New York Times.* September 22, 2015 *(https://www.nytimes.com/2015/09/23/nyregion/volkswagens-diesel-fraud-makes-critic-of-secret-code-a-prophet.html).*

[58] Ambassador Tai. 2021 *(https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2021/november/remarks-ambassador-katherine-tai-digital-trade-georgetown-university-law-center-virtual-conference).*

[59] USMCA Art. 19.16.1; U.S.-Japan Art. 17.

[60] USMCA Art. 19.1; U.S.-Japan Art. 1.

[61] Slok-Wódkowska and Mazur. 2022 at 98 *(https://academic.oup.com/jiel/article/25/1/91/6534278).*

[62] USMCA Art. 19.16.2; U.S.-Japan Art. 17.

[63] McCann. 2019 at 15 *(https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf).*

[64] AI NOW Institute. "2019 Report." December 2019 at 10 *(https://ainowinstitute.org/AI_Now_2019_Report.pdf).*

[65] Bernhardt, Kresge and Suliman. 2021 at 2 *(https://laborcenter.berkeley.edu/data-algorithms-at-work/).*

[66] Mearian, Lucas. "The rise of digital bosses: They can hire you—and fire you." *Computerworld.* January 6, 2022 *(https://www.computerworld.com/article/3646234/the-rise-of-ai-based-managers-they-now-play-a-big-role-in-hiring-training-and-firing.html);* Finnegan, Matthew. "EU 'gig worker' rules look to rein in algorithmic management." *Computerworld.* December 15, 2021 *(https://www.computerworld.com/article/3644462/eu-gig-worker-rules-look-to-rein-in-algorithmic-management.html).*

These automated workplace systems harm workers. A 2021 review of 45 studies on algorithmic management found that more than 90 percent of them highlighted the negative impacts on workers, from de-skilling and task variety, lower worker autonomy and increased workplace control, and increased work intensity and job insecurity.[67] Algorithmic management software are "black box" unaccountable systems that hide what data is relied upon and how the data is used to make decisions. The lack of transparency can obscure the harms which are likely to proliferate as these technologies become more widely implemented.

The digital trade source code and algorithm provisions could make it harder for governments to protect workers from unfair and illegal labor practices, to enforce current law, or to address emerging worker protection issues, including:

- *Enforcing workplace safety laws against productivity-prodding algorithmic management that can increase injury rates:* Workplace surveillance and algorithmic management can impose productivity targets that can lead to workplace injuries. Amazon warehouse workers are monitored by artificial intelligence-enhanced security cameras and handheld package scanners that track worker movements and evaluate work speed and can even terminate workers based on data collected on workplace productivity metrics.[68] Workers believe that maintaining a high package pick rate is essential to getting permanent or better positions, creating strong incentives to increase work intensity.[69] Workers have been disciplined and even fired for failing to hit pick-rate productivity targets.[70] Amazon's warehouse worker productivity programs have ratcheted up workloads and work speed and are associated with the company's injury rate that is three times the national average, with serious injury rates five times the national average.[71] The Occupational Safety and Health Administration should be able to assess the extent that algorithmic productivity software is increasing workplace injuries.
- *Algorithmic surveillance of workers personal social media presence stifles right to form unions:* Some employers are snooping on workers' social media accounts to find unfavorable opinions of the company as well as determine worker discontent and union sympathies. About half of large employers use software to analyze the text of employee social media posts, according to a 2018 survey.[72] A 2022 memo from the National Labor Relations Board general counsel stated that "omnipresent surveillance and other algorithmic-management tools" can "significantly impair" the right to form or join unions.[73] There are many examples of anti-union worker surveillance. Amazon's Whole Foods has used heat maps and predictive algorithms to track locations that were estimated to be high-risk for union activity.[74] McDonalds has operated an intelligence team that monitored the Fight for $15 organizers, which McDonalds employees were active in the campaign, and which

---

[67] Parent-Rocheleau, Xavier and Sharon K. Parker. "Algorithms as work designers: How algorithmic management influences the design of jobs." *Human Resource Management Review*. May 2021 *(https://www.sciencedirect.com/science/article/abs/pii/S1053482221000176?via%3Dihub).*

[68] Constantz, Jo. (Constanz). "'They Were Spying on Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions." *Newsweek*. December 13, 2021 *(https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603);* Wood, Alex J. (Wood). European Commission. Joint Research Center. "Algorithmic Management: Consequences for Work Organisation and Working Conditions." JCR Working Paper No. 124874. 2021 at 8 to 9 *(https://joint-research-centre.ec.europa.eu/system/files/2021-05/jrc124874.pdf).*

[69] Wood. 2021 at 7 *(https://joint-research-centre.ec.europa.eu/system/files/2021-05/jrc124874.pdf).*

[70] Dastin, Jeffrey. "Amazon issued 13,000 disciplinary notices at a single U.S. warehouse." Reuters. July 12, 2022 *(https://www.reuters.com/technology/amazon-issued-13000-disciplinary-notices-single-us-warehouse-2022-07-12/).*

[71] Athena Coalition. "Packaging Pain: Workplace Injuries in Amazon's Empire." January 10, 2020 *(https://www.nelp.org/publication/packaging-pain-workplace-injuries-amazons-empire/).*

[72] Gartner. "The Future of Employee Monitoring." May 3, 2019 *(https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring).*

[73] Abruzzo, Jennifer A. General Counsel. National Labor Relations Board. Office of the General Counsel. "Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights." Memorandum No. GC–23–02. October 31, 2022 at 1 *(https://apps.nlrb.gov/link/document.aspx/09031d45838de7e0).*

[74] Constantz. December 13, 2021 *(https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603).*

workers and locations were interested in forming unions.[75] The meal kit company HelloFresh used software to mine social media posts on Twitter and Instagram looking for content about unionization efforts and identify whether the posts belonged to an employee.[76] The Labor Department should be able to determine whether this kind of algorithmic surveillance violates the right to form or join unions.

- *Automated scheduling software can violate labor law and shortchange workers:* Retail companies use algorithms to automate just-in-time shift schedules to minimize costs that often leave workers without stable work schedules that reduce economic stability and disrupt family life.[77] Half of retail workers face uncertain scheduling that compounds the economic precarity from low wages.[78] Retail workers under algorithmic scheduling can receive shorter hours, on-call shifts that never materialize, or shift assignments without prior notice.[79] The adoption of one algorithmic scheduling software can convert full-time workers into part-time workers, ending their health-care coverage.[80] Algorithmic scheduling software can also encourage managers attempting to meet productivity targets to press workers to work off the clock, skip breaks, or misattribute paid sick leave that can amount to wage theft.[81] Government authorities need to be able to access source code to assess how algorithmic scheduling can negatively affect workers and potentially violate wage and hour law.
- *Artificial intelligence recruiting and hiring tools run afoul of civil rights and employment law:* Employers are increasingly using artificial intelligence-driven tools to recruit, screen, rank, and assess candidates' interview performances which in turn is affecting prospective workers' chances of getting hired.[82] More than two-thirds of human resources leaders and recruiters were using artificial intelligence tools to automate recruiting and hiring.[83] These systems can entrench the existing subjective preferences that perpetuate racial and social biases that contribute to occupational segregation and racial, gender, and economic inequality.[84] The data-driven systems purport to be objective and logical but often have built in biases and rely on faulty data inputs that amplify the detrimental impacts on workers.[85] Some automated applicant screening processes have made it harder for people with non-white sounding or foreign sounding names, women, older people, or people with disabilities to be interviewed and get a chance at a job.[86] As evidence mounts, the discriminatory impact of these artificial intelligence screening and hiring

---

[75] Franceshi-Bicchierai, Lorenzo and Lauren Kaori Gurley. "McDonald's Secretive Intel Team Spies on 'Fight for $15' Workers, Internal Documents Show." *Vice.* February 24, 2021 *(https://www.vice.com/en/article/pkdkz9/mcdonalds-secretive-intel-team-spies-on-fight-for-15-workers).*

[76] Kaori Gurley, Lauren. "Internal Slacks Show HelloFresh Is Controlling Talk of Unionization." *Vice.* November 19, 2021 *(https://www.vice.com/en/article/n7nb9w/internal-slacks-show-hellofresh-is-controlling-talk-of-unionization).*

[77] Finnegan, Matthew. "EU 'gig worker' rules look to rein in algorithmic management." *Computerworld.* December 15, 2021 *(https://www.computerworld.com/article/3644462/eu-gig-worker-rules-look-to-rein-in-algorithmic-management.html);* Wykstra, Stephani. "The movement to make workers' schedules more humane." *Vox.* November 5, 2019 *(https://www.vox.com/future-perfect/2019/10/15/20910297/fair-workweek-laws-unpredictable-scheduling-retail-restaurants).*

[78] Schneider, Daniel and Kristen Harknett. University of California Berkeley and Aspen Institute. "Income Volatility in the Service Sector: Contours, Causes, and Consequences." July 2017 at 2 *(http://www.aspenepic.org/wp-content/uploads/2017/07/ASPEN_RESEARCH_INCOME_VOLATILITY_PRINT.pdf).*

[79] Kaplap, Esther. (Kaplap). "The Spy Who Fired Me." *Harper's Magazine.* March 2015 *(https://harpers.org/archive/2015/03/the-spy-who-fired-me/).*

[80] Wood. 2021 at 4 *(https://joint-research-centre.ec.europa.eu/system/files/2021-05/jrc124874.pdf).*

[81] Kaplap. March 2015 *(https://harpers.org/archive/2015/03/the-spy-who-fired-me/).*

[82] Yang. 2020 at 3 and 4 *(https://edworkforce.house.gov/download/jenny-r-yang/default.aspx).*

[83] Ajunwa, Ifeoma. (Ajunwa). Cornell University Industrial and Labor Relations School. Statement before the Subcommittee on Civil Rights and Human Services. Committee on Education and Labor. U.S. House of Representatives. "The Future of Work: Protecting Workers' Civil Rights in the Digital Age." February 5, 2020 at 3 *(https://edworkforce.house.gov/download/ifeoma-anunwa/default.aspx).*

[84] Yang. 2020 at 4 to 5 *(https://edworkforce.house.gov/download/jenny-r-yang/default.aspx).*

[85] *Ibid.* at 1.

[86] Ajunwa. 2020 at 5 to 6 *(https://edworkforce.house.gov/download/ifeoma-anunwa/default.aspx);* Yang. 2020 at 4 *(https://edworkforce.house.gov/download/jenny-r-yang/default.aspx).*

processes are being challenged as potential violations of civil rights and anti-discrimination laws.[87]

- *Algorithmic management of gig workers suppresses earnings:* Algorithmic management of gig workers erodes workers' economic security by assigning tasks or suppressing earnings through pricing algorithms that can overwork and underpay gig workers. Gig drivers are often paid under algorithmic rates that use secret calculations to set fares and charges that have tended to suppress earnings.[88] *The Washington Post* reported that changes to pay rate algorithms pushed earnings down by as much as 50 percent for the same number of hours and trips.[89] Platform companies also use algorithms to discipline or block gig workers from jobs. Algorithms can wrongly downgrade workers or suspend their accounts without disclosing the alleged misdeeds or providing a remedy.[90] These platform "deactivations" amount to short-term termination by algorithm that reduces earnings.[91] The combination of platform algorithmic evaluation and discipline pushes workers to work intensively for long hours without a break.[92]
- *Automated surveillance of workers undermines privacy and workers' rights:* Employers are increasingly deploying advanced surveillance to monitor workers on the job and even outside the workplace.[93] The declining cost of worker surveillance has been supercharged by artificial intelligence systems that have made surveillance more prevalent and includes digital cameras, productivity monitoring applications, key card and RFID tracking, wearable electronic monitors, geolocating and heat sensory tracking, keystroke logging, WIFI network logs, wellness programs, biometrics, and monitoring workers' Internet search and social media activity.[94] This surveillance is often unknown to workers and companies need not receive workers' consent; the surveillance data is owned by the employer which can share or sell this data without workers' approval.[95]

A worker-centered digital trade agenda must provide meaningful public policy space to address the impacts of automated decision-making and algorithmic management on workers and society: The rise of automated decision-making and artificial intelligence-driven algorithms poses new challenges to enforce current laws and to address emerging and novel issues that affect workers and society. The digital trade source code and algorithm provisions could make it harder for government to take decisive steps to address existing and new problems driven by these technologies. A worker-centered trade agenda would provide sufficient policy space to address these technological challenges. This should include addressing the corrosive effect that social media algorithms are having on democracy, civil discourse, and the mental health of young people as well as the monopolistic power exerted by platform and e-commerce behemoths. The public policy space to protect workers should include, at a minimum:

- *Meaningful oversight of source codes and algorithms to ensure compliance with labor and employment laws:* Governments must be able to examine cor-

---

[87] Opfer, Chris. "AI Hiring Could Mean Robot Discrimination Will Head to Courts." *Bloomberg Law.* November 12, 2019 *(https://news.bloomberglaw.com/daily-labor-report/ai-hiring-could-mean-robot-discrimination-will-head-to-courts).*

[88] Feliz Leon, Luis. "How Gig Workers in Canada Are Fighting for Employee Rights." *The Real News.* March 8, 2022 *(https://therealnews.com/how-gig-workers-in-canada-are-fighting-for-employee-rights).*

[89] Bhattarai, Abha. "'Don't game my paycheck': Delivery workers say they're being squeezed by ever-changing algorithms." *Washington Post.* November 7, 2019 *(https://www.washingtonpost.com/business/2019/11/07/dont-game-my-paycheck-delivery-workers-say-theyre-being-squeezed-by-ever-changing-algorithms/).*

[90] Murgia, Madhumita. "Workers demand gig economy companies explain their algorithms." *Financial Times.* December 13, 2021 *(https://www.ft.com/content/95e7f150-b0f9-4602-8e5d-76a138b59851).*

[91] Kaori Gurley, Lauren. "Workers Need to Unionize to Protect Themselves From Algorithmic Bosses." *Vice.* December 19, 2019 *(https://www.vice.com/en/article/epg4b4/workers-need-to-unionize-to-protect-themselves-from-algorithmic-bosses).*

[92] Wood. 2021 at 10 *(https://joint-research-centre.ec.europa.eu/system/files/2021-05/jrc124874.pdf).*

[93] Ajunwa, Crawford, and Schultz. 2017 at 738 to 739 *(https://californialawreview.org/print/3-limitless-worker-surveillance/).*

[94] *Ibid.;* Abril, Danielle. "Your boss can monitor your activities without special software." *Washington Post.* October 7, 2022 *(https://www.washingtonpost.com/technology/2022/10/07/work-app-surveillance/).*

[95] Bernhardt, Kresge and Suliman. 2021 at 18 *(https://laborcenter.berkeley.edu/data-algorithms-at-work/).*

porate source codes, algorithms, and other tools of "AI management" to fully understand their impacts and 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.

- *Policy space to address emerging threats to workers' privacy, including employer use of workplace surveillance software:* The digital trade data provisions only protect the personal data of the "users of digital trade,"[96] which in the context of worker privacy is likely the employer that collects and owns the data and information collected by work-site surveillance. Governments must have the policy space to take measures to address digital workplace surveillance and other emerging threats to workers' privacy.
- *Addressing abusive employment practices in the technology sector:* Large technology and platform companies have promoted an exploitative employment model based on rampant employment misclassification and the outsourcing of core job functions. Platform gig workers are employed as precarious contractors without 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 clean up the labor abuses in their own operations and their digital supply chains, including the ghost workers in the developing world.

IV. OTHER DIGITAL PROVISIONS PRESENT CHALLENGES TO WORKERS AND SOCIETY

The existing digital trade provisions grant broad rights to technology firms with limited protections for people and workers. Beyond the cross-border data and source code provisions, workers can be negatively impacted by the failure to protect copyrighted material and the weak protections against cyberattacks.

Digital trade provisions fail to protect and promote the economic security of creative professionals in the U.S. motion picture, television, and music industries: The digital trade provisions shield platform companies from responsibility for the third-party content posted on their networks that leaves workers in the creative industries vulnerable to copyright infringement that undermines their economic security. The USMCA and U.S.-Japan agreements both absolve suppliers of interactive computer services from "liability for harms related to information stored, processed, transmitted, distributed, or made available by the service."[97] This language mirrors the Digital Millennium Copyright Act language that excludes Internet service providers from being held responsible as a publisher of content on their networks.[98] This absolves platforms and social media companies from responsibility from users promoting hate speech,[99] political disinformation,[100] or other content that has increasingly been associated with negative mental health impacts.[101]

These provisions also harm the more than 4 million people who work in the motion picture, television, and music industries. Many of these workers collectively bargain for payments and contributions to their health insurance and pension plans that are directly tied to the sales and licensing of the copyrighted works that they help create.[102] This content contributes more than $500 billion to the U.S. economy annually and generates a trade surplus.[103] Stolen or unlicensed use of copyrighted

---

[96] USMCA Art. 19.8.2; U.S.-Japan Art. 15.1.

[97] USMCA Art. 19.17.2; U.S.-Japan Art. 18.2.

[98] The Digital Millennium Copyright Act of 1998. 17 U.S.C. § 512.

[99] Castaño-Pulgarín, Sergio Andrés et al. "Internet, social media and online hate speech. Systemic review." *Aggression and Violent Behavior.* Vol 58. 2021 *(https://prohic.nl/wp-content/uploads/2021/05/213-17mei2021-InternetOnlineHateSpeechtSystematicReview.pdf).*

[100] Hiaeshutter-Rice, Dan, Sedona Chinn, and Kaiping Chen. "Platform Effects on Alternative Influencer Content: Understanding How Audiences and Channels Shape Misinformation Online." *Frontiers in Political Science.* May 31, 2021 *(https://www.frontiersin.org/articles/10.3389/fpos.2021.642394/full).*

[101] Twenge, Jean M. et al. "Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time." *Clinical Psychological Science.* Vol. 6, Iss. 1. November 14, 2017 *(https://journals.sagepub.com/doi/10.1177/2167702617723376).*

[102] AFL–CIO. Department for Professional Employees. [Fact sheet]. "Creative Professionals Depend on Strong Copyright Protection." October 4, 2021 *(https://static1.squarespace.com/static/5d10ef48024ce300010f0f0c/t/615b42671fca1314b3ae3048/1633370727780/Copyright+one+pager.pdf).*

[103] AFL–CIO. Department for Professional Employees. [Fact sheet]. "Intellectual Property Theft: A Threat to Working People and the Economy." October 25, 2021 *(https://static1.*

content on digital platforms directly harms these workers, severely diminishing the payment and benefit contributions they have bargained for and the ability of their employers to finance future content creation. Digital trade policy must aggressively address the stolen or unlicensed use of copyrighted content on digital platforms that directly harms these workers.

Protect workers and unions from cyber-crime by both state and private actors: The USMCA and U.S.-Japan digital agreements recognize the importance of protecting networks and users from cyber-crimes to prevent the erosion of confidence in digital trade.[104] Neither provision acknowledges the impact on workers, people, unions, or other organizations that may be harmed by cyber-breaches, malware, ransomware, or other cyber-crimes. The digital trade provisions discourage regulatory approaches to bolster cybersecurity and explicitly promote voluntary "risk-based approaches that rely on consensus-based standard and risk management best practices" to protect against cyber-crimes and respond to cybersecurity events.[105]

Workers and unions can be significantly impacted by cyber-breaches and ransomware attacks that harm unions, expose workers' personal data, and affect their earnings if employers are temporarily shut down. In 2014, the United States charged members of the Chinese military with hacking U.S.-based companies and the United Steelworkers.[106] In 2019, the International Brotherhood of Teamsters was subject to a ransomware attack demanding $2.9 million that forced the union to rebuild its computer servers.[107] Cyberattacks against employers can leave workers vulnerable to unexpected shutdowns and shift cancellations, as happened to unionized meatpacking workers in 2021.[108] The United Food and Commercial Workers International Union was able to secure pay for workers that lost shifts to the cyber-attack, but these types of attacks could cost workers' shifts and income if employers are forced to idle facilities or business locations. A cyber-breach against an entertainment payroll company potentially exposed the personal information and bank accounts of Screen Actors Guild–American Federation of Television and Radio Artists members in 2014.[109] Digital trade policy must strive to improve cybersecurity and create a common enforcement agenda to hold the criminals and companies that facilitate these crimes accountable.

V. CONCLUSION

As the Biden administration continues to remake U.S. trade policy, 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 interests of big technology companies.

Too often, the debate over digital trade is framed as a binary choice between authoritarian digital censorship or the unregulated status quo that leaves big tech free to collect, control, and commodify workers and consumers' private data as they see fit. The labor movement rejects this false choice. Digital trade rules cannot grant broad powers to big tech and prevent governments from protecting workers from the downsides of the digital transformation of the economy.

It is time for a strategic re-set on digital trade policy. The public, including workers and labor unions, must decide the rules of the road for technology in the workplace and society. There must be a new democratic, stakeholder-driven approach to

---

squarespace.com/static/5d10ef48024ce300010f0f0c/t/6177099c283f42475e62bc77/16351911 96820/2021+IP+theft+fact+sheet.pdf).

[104] USMCA Art. 19.15.1; U.S.-Japan Art. 15.1.

[105] USMCA Art. 19.15.2; U.S.-Japan Art. 1.2.

[106] Miller, John. W. "Pittsburgh-Area Firms Allegedly Targeted by Hackers." *Wall Street Journal.* May 19, 2014 *(https://www.wsj.com/articles/SB10001424052702304422704579572273980 220140);* U.S. Department of Justice. [Press release]. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." May 19, 2014 *(https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and).*

[107] Allen, Jonathan and Kevin Collier. "Ransomware attack hits Teamsters in 2019—but they refused to pay." NBC News. June 11, 2021 *(https://www.nbcnews.com/tech/security/ransomware-attack-hit-teamsters-2019-they-refused-pay-n1270461).*

[108] "Fallout and Blame: Ransomware Attack Against World's Largest Meat Producer." *SecureWorld News.* June 1, 2021 *(https://www.secureworld.io/industry-news/cyberattack-global-meat-producer).*

[109] Raman, Jeffrey. "Entertainment Payroll Firm Breached." *BankINfo Security.* December 4, 2014 *(https://www.bankinfosecurity.com/entertainment-payroll-firm-breached-a-7639);* SAG–AFTRA. [Press release]. "An Important Announcement About ART Payroll." December 2, 2014 *(https://www.sagaftra.org/important-announcement-about-art-payroll).*

data governance that confronts the negative impacts of digitization on workers, consumers, and society.

The Biden administration's call for a 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.

COMMUNICATIONS

CENTER FOR FISCAL EQUITY
14448 Parkvale Road, Suite 6
Rockville, MD 20853
fiscalequitycenter@yahoo.com

Statement of Michael G. Bindner

Chairman Carper and the Ranking Member Cornyn, thank you for the opportunity to submit these comments for the record to the Subcommittee on International Trade, Customs, and Global Competitiveness. These comments are in reaction to the submitted testimony, and would have dealt with the same issues, regardless, as evidenced by the amount of material reused from previous comments to both revenue committees and trade subcommittees.

That the Global South was ignored by the subcommittee and the witnesses is troubling. For these nations, the digital economy will include distance learning modalities. While the SpaceX Starlink constellation has been criticized as not being affordable for most people, a village or neighborhood could be given a shared link and server.

Distance learning could include STEM, more advanced language proficiency and a more realistic look at American civic culture in all of its gore. The way Black and Brown people are really treated may stem the drive to leave home for a life of low wage labor in America.

In June of this year, we highlighted the fact that the next labor market to be tapped is Africa. As Asian labor markets mature, capitalists will seek cheaper workers. American trade policy should step in to train workers before WalMart's supply chain arrives. From June, historically . . .

> . . . capitalist firms would set up factories in developing nations with excess labor forces (usually due to modernization of agriculture or rent seeking by landed elites) and pay the workers as cheaply as possible. It is the messy way to industrialize. It seems to work, but it carries human costs while workers gather the leverage to organize and the power to increase domestic demand by consumption. Both of these factors increase wages.
>
> We need not be messy about assisting the Motherland on its road to industrialization. As capitalism moves toward establishing a foothold in Africa, our trade policy must be ready to insist on the right of African workers to organize, partnered with the American labor movement in helping them to do so. We can partner with American colleges to establish campuses in sub-Saharan Africa so that their best and brightest need not come to us. We can come to them.
>
> Technical assistance on employee ownership (which is still emergent in the United States), as well as in the creation of property rights for farmers, is essential. Finally, we can assist Africa in creating commodity futures markets of their own so that farmers can obtain working capital by selling futures and decide whether it is in their interest to sell food abroad. The natural progress toward industrialization is not inevitable. It can move past exploitation without stopping there.

The Ranking Member's opening statement is correct, the Administration should begin working on restarting a Trans-Pacific Partnership. It was ill-advised for Secretary Clinton to take it off the table in response to its rejection by the Stable Genius who pressed the issue, just to refresh all of our memories of why TPP was dropped.

Much of our supply chain difficulties come from the trade war started by the prior Administration, although the current administration does own its continued existence by not acting to reverse Trump's petulance. In June 2019, we characterized

> trade negotiations with China, Japan, the EU, and the UK threatening tariffs have taken on the character of economic gunboat diplomacy, but without the Navy. These occur because the President is ill equipped by his background as a businessman to work cooperatively, which is the essence of governance in a free society. He has a freer hand in trade negotiations. Sadly, his experience as a CEO has not served the nation well. The modus operandi of most executives is to break things in order to be seen fixing them. This must stop. The public is not amused, including the Chamber of Commerce, farmers and the stock and commodity markets.

In March of 2020, we stated that "recent developments indicate that Amateur Hour at the White House over trade policy has ended. Our naked emperor has moved on to self-defense, allowing the adults to put things back together again."

On the security front, the "digital mercantilism" of China is troubling, however, it will not last. The Party has backed down on its Zero COVID policy, but victory in the streets traditionally means that taking it to the streets has begun to work. It is a heady thing. There is no putting the genie back in the bottle. Not in China, not in Iran, not in post George Floyd America.

In each case, today's protesters and revolutionaries will become the backbone of the next revolution. For example, when the Civil Rights revolution made its way to the District of Columbia in 1968, it stayed to both end discrimination and move toward home rule. While most of that generation has retired or passed on, the District's delegate is still going strong.

Again, to repeat prior comments, "China is still firmly under the control of their Communist Party and membership still has its privileges, but the entrepreneurial spirit unleashed there has morphed into revolution. Their AI industry is often with the support of American expatriates. It is now surpassing what we can do. Research has or will soon surpass American progress. China may soon begin talking about our problems in protecting intellectual property, which are numerous."

Let us hope that our Expats also teach Democracy as well as they teach business.

Economic progress in China is not terribly different from the progress of economic and political freedom in the Global North of the Western World. While a Marxist revolution has never occurred in a Marxist state, a Marxian analysis (not the elevator speech that Stalin and Mao implemented), society moves forward in largely predictable ways.

Aristocracy (or Party) brings about industrialization under a capitalistic despotism, which includes militarism and imperialism. As the peasantry is forced into slave like conditions in urban factories, they soon acquire skills and savings. Eventually, they demand civil and union rights, which their capitalist masters resist until a consumer surplus is required to match the labor surplus, usually because production exceeds worker income.

Until the revolution occurs, and even after it does, current history has proven our digital vulnerability. It is simply unwise to keep the public Internet and the Internet of Technology on the same system.

When I was a cost analyst with the United States Air Force, we had a dedicated line from the Air Force Finance and Accounting System in Colorado Springs. This was before the world wide web, but was likely part of the single system. More recently, as a contract administrator at the Department of Energy, we worked out a deal with our providers to allow Verizon to keep control of connections within buildings, while competing what is called "pipe" from buildings to data centers.

To create a TechNet, it is better to keep physical connections separate rather than trying to program fire walls. In other places, we have proposed creating a network of overhead power and digital connectivity for electric vehicles, ending the need to further develop lithium ion batteries or self-driving cars. Such a system must separate system communication with Internet communication so that the system cannot be hacked, all the while letting passengers watch CNN, Fox News or Netflix on the way to their destinations. This infrastructure would also provide power to homes, factories and offices.

The next issue is the international use of Big Data, including the one-sided treatment in China where they see ours, but do not show theirs. I will further discuss

issues of data privacy below, when discussing employee ownership as an alternative to international labor agreements. For now, it is important to make a distinction.

Some data is intellectual property to be used in creating a product or service. Other digital technology is the product, for example, the reading of an X-Ray by a South Asian doctor working from home. This work is for pay, so the question is the taxation of internationally provided services generally, as well as physical products. Readers familiar with the Center's previous comments know where I am taking this from here on out.

The United States, in refusing to adopt consumption taxes, has cut off its nose to spite its face. Under the credit invoice VAT regime, imported goods and services would lose their VAT burden for what they export, with the importing nation adding their own VAT at import. Doing so ends the permanent disadvantage faced by American workers and small businesses and eliminates the ability of our new Billionaire Class to borrow against their fortunes to avoid taxation while consuming high-end goods and creating new ventures.

This should become an electoral issue, or rather, a campaign finance issue. It would evaporate with public campaign finance. Current fundraising is the biggest obstacle to real tax reform. Until a candidate focuses on tax reform the way that Governor Huckabee senior focused on the Fair Tax, bipartisan corruption will continue and the working class will continue to lose ground.

As usual, we have included an attachment on how trade would occur in a VAT-based system. Goods and services taxes would fund general government and what was the employer contribution to Social Security (which would from then on be credited on an equal dollar basis rather than a dollar-for-dollar match). A subtraction VAT on employer labor and profit will fund services to employees and their families (health care and the child tax credit federally, education and social welfare at the state level).

As part of American entry into modern taxation as practiced by the rest of the Organization for Economic Cooperation and Development, we can negotiate which taxes are used to fund which activities on a global basis. No member state should try to push all of its social costs onto importers because some of these costs benefit worker families—which is part of doing business in a just economy. The importer benefits from such systems and should pay for them. Discretionary spending and retirement taxation, however, can be shed at the border.

To make sure that taxes are collected in the digital economy when due, especially regarding the use of Big Data in marketing and manufacturing, those who purchase or use it must be required to buy a license to do so. This will allow for investigation of how such data is used or misused and whether it is taxed correctly. In a VAT based system, imported data that arrives as a product rather than a component would be taxed on entry, but not as enterprise data.

Corporate income taxes would be abolished in this system. This will end all of the concerns about taxing intellectual property within an enterprise. As long as goods and services are taxed appropriately when consumed (both by invoice and subtraction VAT), the United States can be agnostic on where patents are held. The recently enacted corporate minimum tax would thus be repealed. Sadly, the current opposition was party politics and ignored the fact that this tax was enacted as part of a larger agreement by the OECD. We signed it, we ratified it and repealing it must be international.

Please see the second attachment regarding our Asset Value Added Tax proposal, which comes from our usual tax reform attachment and comments provided to the revenue committees in their consideration of the Treasury Department Budget earlier this year. Note that there have been updates to proposed rates based on recent analyses and the need for compromise due to the recent election.

Instead of negotiated minimum tax agreements in the OECD, agreements would be negotiated on Asset VAT rates. These should be uniform to prevent market shopping and revenues could be dedicated to such items as common defense (including the United States Navy, etc.) and international debt forgiveness (to square the circle drawn in the first section on Africa).

The AFL–CIO's comments are not to be taken lightly, although playing catch up does not seem to be working well. It is time to shift from adversarial bargaining to the kind of representation that would take place where unions and professional organizations in a company hold the voting proxies of their members at shareholder

meetings of employee-owned companies. Such meetings will replace unitary boards of directors.

Our second and third attachments from June 2022 and July 2019 provide detail on the advantages of employee ownership, both here and abroad. In brief, employee-owned firms would expand their ownership structures to overseas subsidiaries and to its current supply chain. Transfer pricing would be based on a common market basket of employee-purchased goods rather than currency arbitrage.

This would likely require some modification to laws on both trade and fiduciary rules. Taft-Hartley limitations on how much of an employing firm a union pension fund can own must also be revised. Zero rating asset VAT sales to broad based ESOP and cooperative enterprises is also necessary to end cross-border worker exploitation.

Aside from retention of capitalistic management structures, rather than cooperative ones, a big reason that ESOPs have not been more widely sought is the lack of additional cash and prizes. In the United States, such firms rarely challenge the implicit assumption that household consumption and finance is left to the household rather than provided cooperatively. (This is not the case with some overseas trade unions or cooperatives such as Mondragon).

Not asking the question of whether common consumption, housing and finance systems should be considered is its own answer. If the question were actually asked, after informing employee owners of what is possible, the free market will have workers flock to these firms—especially in our post-COVID, broken supply chain world. If your company sells you housing where you can grow your own vegetables and lab-grown protein, prices never go up.

One advantage of employee and cooperative ownership would deal with the problem of "Big Data." Employee-controlled financial and consumption systems will not sell their data or let their suppliers do so. Solving these issues will also defuse our constant arguments on economics and on which party is "winning." We can begin to live together again as neighbors and friends, rather than being manipulated by an increasing hostile social media space.

Thank you for this opportunity to share these ideas with the committee. As always, we are available to meet with members and staff or to provide direct testimony on any topic you wish.

Attachment—Trade Policy and Value-Added Taxes

Consumption taxes could have a big impact on workers, industry and consumers. Enacting an I–VAT is far superior to a tariff. The more government costs are loaded onto an I–VAT the better. If the employer portion of Old-Age and Survivors Insurance, as well as all of disability and hospital insurance are decoupled from income and credited equally and personal retirement accounts are not used, there is no reason not to load them onto an I–VAT. This tax is zero rated at export and fully burdens imports.

Seen another way, to not put as much taxation into VAT as possible is to enact an unconstitutional export tax. Adopting an I–VAT is superior to its weak sister, the Destination Based Cash Flow Tax that was contemplated for inclusion in the TCJA. It would have run afoul of WTO rules on taxing corporate income. I–VAT, which taxes both labor and profit, does not.

The second tax applicable to trade is a Subtraction VAT or S–VAT. This tax is designed to benefit the families of workers through direct subsidies, such as an enlarged child tax credit, or indirect subsidies used by employers to provide health insurance or tuition reimbursement, even including direct medical care and elementary school tuition. As such, S–VAT cannot be border adjustable. Doing so would take away needed family benefits. As such, it is really part of compensation. While we could run all compensation through the public sector.

The S–VAT could have a huge impact on long term trade policy, probably much more than trade treaties, if one of the deductions from the tax is purchase of employer voting stock (in equal dollar amounts for each worker). Over a fairly short period of time, much of American industry, if not employee-owned outright (and there are other policies to accelerate this, like ESOP conversion) will give workers enough of a share to greatly impact wages, management hiring and compensation and dealing with overseas subsidiaries and the supply chain—as well as impacting certain legal provisions that limit the fiduciary impact of management decision to improving short-term profitability (at least that is the excuse managers give for not privileging job retention).

Employee owners will find it in their own interest to give their overseas subsidiaries and their supply chain's employees the same deal that they get as far as employee ownership plus an equivalent standard of living. The same pay is not necessary, currency markets will adjust once worker standards of living rise.

Over time, ownership will change the economies of the nations we trade with, as working in employee-owned companies will become the market preference and force other firms to adopt similar policies (in much the same way that, even without a tax benefit for purchasing stock, employee-owned companies that become more democratic or even more socialistic, will force all other employers to adopt similar measures to compete for the best workers and professionals).

In the long run, trade will no longer be an issue. Internal company dynamics will replace the need for trade agreements as capitalists lose the ability to pit the interest of one nation's workers against the others. This approach is also the most effective way to deal with the advance of robotics. If the workers own the robots, wages are swapped for profits with the profits going where they will enhance consumption without such devices as a guaranteed income.

Asset VAT—The President's Fiscal Year 2023 Budget, June 7, 2022

There are two debates in tax policy: how we tax salaries and how we tax assets (returns, gains and inheritances). Shoving too much into the Personal Income Tax mainly benefits the wealthy because it subsidizes losses by allowing investors to not pay tax on higher salaries with malice aforethought.

Asset Value-Added Tax (A–VAT) is a replacement for capital gains taxes and the estate tax. It will apply to asset sales, exercised options, inherited and gifted assets and the profits from short sales. Tax payments for option exercises, IPOs, inherited, gifted and donated assets will be marked to market, with prior tax payments for that asset eliminated so that the seller gets no benefit from them. In this perspective, it is the owner's increase in value that is taxed.

As with any sale of liquid or real assets, sales to a qualified broad-based Employee Stock Ownership Plan will be tax free. This change would be counted as a tax cut, giving investors in public stock who make such sales the same tax benefit as those who sell private stock.

This tax will end Tax Gap issues owed by high income individuals. The base 20% capital gains tax has been in place for decades. The current 23.8% rate includes the ACA–SM surtax), while the Biden proposal accepted by Senator Sinema is 28.8%. Our proposed Subtraction VAT would eliminate the 3.8% surtax. This would leave a 25% rate in place.

Settling on a bipartisan 22.5% rate (give or take 0.5%) should be bipartisan and carried over from the capital gains tax to the asset VAT. A single rate also stops gaming forms of ownership. Lower rates are not as regressive as they seem. Only the wealthy have capital gains in any significant amount. The de facto rate for everyone else is zero.

With tax subsidies for families shifted to an employer-based subtraction VAT, and creation of an asset VAT, taxes on salaries could be filed by employers without most employees having to file an individual return. It is time to *tax transactions, not people!*

The tax rate on capital gains is seen as unfair because it is lower than the rate for labor. This is technically true, however it is only the richest taxpayers who face a marginal rate problem. For most households, the marginal rate for wages is less than that for capital gains. Higher income workers are, as the saying goes, crying all the way to the bank.

In late 2017, tax rates for corporations and pass-through income were reduced, generally, to capital gains and capital income levels. This is only fair and may or may not be just. The field of battle has narrowed between the parties. The current marginal and capital rates are seeking a center point. It is almost as if the recent tax law was based on negotiations, even as arguments flared publicly. Of course, that would never happen in Washington. Never, ever.

Compromise on rates makes compromise on form possible. If the Affordable Care Act non-wage tax provisions are repealed, a rate of 26% is a good stopping point for pass-through, corporate, capital gains and capital income.

A single rate also makes conversion from self-reporting to automatic collection through an asset value-added tax levied at point of sale or distribution possible. This would be both just and fair, although absolute fairness is absolute unfairness

to tax lawyers because there would be little room to argue about what is due and when.

Ending the machinery of self-reporting also puts an end to the Quixotic campaign to enact a wealth tax. To replace revenue loss due to the ending of the personal income tax (for all but the wealthiest workers and celebrities), enact a Goods and Services Tax. A GST is inescapable. Those escapees who are of most concern are not waiters or those who receive refundable tax subsidies. It is those who use tax loopholes and borrowing against their paper wealth to avoid paying taxes.

For example, if an unnamed billionaire or billionaires borrow against their wealth to go into space, creating such assets would be taxable under a GST or an asset VAT. When the Masters of the Universe on Wall Street borrow against their assets to avoid taxation, having to pay a consumption tax on their spending ends the tax advantage of gaming the system.

This also applies to inheritors. No "Death Tax" is necessary beyond marking the sale of inherited assets to market value (with sales to qualified ESOPs tax free). Those who inherit large cash fortunes will pay the GST when they spend the money or Asset VAT when they invest it. No special estate tax is required and no life insurance policy or retirement account inheritance rules will be of any use in tax avoidance.

Tax avoidance is a myth sold by insurance and investment brokers. In reality, explicit and implicit value-added taxes are already in force. Individuals and firms that collect retail sales taxes receive a rebate for taxes paid in their federal income taxes. This is an intergovernmental VAT. Tax withheld by employers for the income and payroll taxes of their labor force is an implicit VAT. A goods and services tax simply makes these taxes visible.

Should the tax reform proposed here pass, there is no need for an IRS to exist, save to do data matching integrity. States and the Customs Service would collect credit invoice taxes, states would collect subtraction VAT, the SEC would collect the asset VAT and the Bureau of the Public Debt would collect income taxes or sell tax prepayment bonds. See the last attachment for details on this.

Attachment—A. Employee Ownership, March 7, 2019

Employee ownership is the ultimate protection for worker wages. Our proposal for expanding it involves diverting an every-increasing portion of the employer contribution to the Old-Age and Survivors fund to a combination of employer voting stock and an insurance fund holding the stock of all similar companies. At some point, these companies will be run democratically, including CEO pay, and workers will be safe from predatory management practices. Increasing the number of employee-owned firms also decreases the incentive to lower tax rates and bid up asset markets with the proceeds.

Establishing personal retirement accounts holding index funds for Wall Street to play with will not help. Accounts holding voting and preferred stock in the employer and an insurance fund holding the stocks of all such firms will, in time, reduce inequality and provide local constituencies for infrastructure improvements and the funds to carry them out.

ESOP loans and distribution of a portion of the Social Security Trust Fund could also speed the adoption of such accounts. Our Income and Inheritance Surtax (where cash from estates and the sale of estate assets are normal income) would fund reimbursements to the Fund.

At some point, these companies will be run democratically, including CEO pay, and workers will be safe from predatory management practices. This is only possible if the Majority quits using fighting it as a partisan cudgel and embraces it to empower the professional and working classes.

The dignity of ownership is much more than the dignity of work as a cog in a machine.

B. From Hearing on the 2016 Social Security Trustees Report

In the January 2003 issue of *Labor and Corporate Governance,* we proposed that Congress should equalize the employer contribution based on average income rather than personal income. It should also increase or eliminate the cap on contributions. The higher the income cap is raised, the more likely it is that personal retirement accounts are necessary. A major strength of Social Security is its income redistribution function. We suspect that much of the support for personal accounts is to sub-

vert that function—so any proposal for such accounts must move redistribution to account accumulation by equalizing the employer contribution.

We propose directing personal account investments to employer voting stock, rather than an index funds or any fund managed by outside brokers. There are no Index Fund billionaires (except those who operate them). People become rich by owning and controlling their own companies. Additionally, keeping funds in-house is the cheapest option administratively. I suspect it is even cheaper than the Social Security system—which operates at a much lower administrative cost than any defined contribution plan in existence.

If employer voting stock is used, the Net Business Receipts Tax/Subtraction VAT would fund it. If there are no personal accounts, then the employer contribution would be VAT funded.

Safety is, of course, a concern with personal accounts. Rather than diversifying through investment, however, We propose diversifying through insurance. A portion of the employer stock purchased would be traded to an insurance fund holding shares from all such employers. Additionally, any personal retirement accounts shifted from employee payroll taxes or from payroll taxes from non-corporate employers would go to this fund.

The insurance fund will save as a safeguard against bad management. If a third of shares were held by the insurance fund than dissident employees holding 25.1% of the employee-held shares (16.7% of the total) could combine with the insurance fund held shares to fire management if the insurance fund agreed there was cause to do so. Such a fund would make sure no one loses money should their employer fail and would serve as a sword of Damocles to keep management in line. This is in contrast to the Cato/PCSSS approach, which would continue the trend of management accountable to no one. The other part of my proposal that does so is representative voting by occupation on corporate boards, with either professional or union personnel providing such representation.

The suggestions made here are much less complicated than the current mix of proposals to change bend points and make OASI more of a needs based program. If the personal account provisions are adopted, there is no need to address the question of the retirement age. Workers will retire when their dividend income is adequate to meet their retirement income needs, with or even without a separate Social Security program.

No other proposal for personal retirement accounts is appropriate. Personal accounts should not be used to develop a new income stream for investment advisors and stock traders. It should certainly not result in more "trust fund socialism" with management that is accountable to no cause but short term gain. Such management often ignores the long-term interests of American workers and leaves CEOs both over-paid and unaccountable to anyone but themselves.

If funding comes through a Subtraction VAT, there need not be any income cap on employer contributions, which can be set high enough to fund current retirees and the establishing of personal accounts. Again, these contributions should be credited to employees regardless of their salary level.

Conceivably a firm could reduce their S–VAT liability if they made all former workers and retirees whole with the equity they would have otherwise received if they had started their careers under a reformed system. Using Employee Stock Ownership Programs can further accelerate that transition. This would be welcome if ESOPs became more democratic than they are currently, with open auction for management and executive positions and an expansion of cooperative consumption arrangements to meet the needs of the new owners.

COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION
25 Massachusetts Avenue, NW, Suite 300C
Washington, DC 20001
Ph: +1 (202) 783–0070
https://ccianet.org/

The Computer and Communications Industry Association (CCIA) submits the following Statement for the Record following the November 30, 2022 Senate Finance Subcommittee on International Trade, Customs, and Global Competitiveness Hearing. CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has pro-

moted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.

CCIA welcomes this opportunity to provide the following recommendations on the U.S. Trade Policy Agenda relating to the digital economy.

The U.S. should continue to negotiate binding commitments in free trade agreements that pertain to digital trade and cross-border delivery of Internet-enabled services. The Digital Trade chapters of the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement represent the gold standard of digital trade provisions, and any agreement pursued by the United States that includes digital trade priorities should reflect those provisions. The United States could also consider new digital trade disciplines and other high-quality digital agreements around the world, such as provisions related to artificial intelligence cooperation found in the Singapore-Australia Digital Economy Agreement. It is clear that our trading partners around the world recognize the importance of getting trade rules for the 21st century right, and it would be a missed opportunity for the United States to delay its engagement on the global stage in forging frameworks that enhance U.S. competitiveness and reflect our values.

At the same time, the United States should not fundamentally overhaul trade policy to undermine the benefits robust trade engagement confers to U.S. industry and consumers. While policymakers are encouraged to reassess approaches to international trade in light of new challenges and the changing global economy, it would be a step backwards to revise these commitments in future agreements that expand exceptions and/or overall weaken the effectiveness of such rules. The United States should continue to pursue high standard agreements that facilitate global commerce, rather than adopting the approach of China in crafting multilateral agreements that have broad exceptions that render commitments meaningless like it is in the case of the Regional Comprehensive Economic Partnership (RCEP). It is important to note that any obligations undertaken are only with respect to partners the United States has chosen, and thus fears that strong rules incentivize trade with or investment in nations whose interests are inimical to ours are misplaced.

Finally, it is also worth noting that IPEF members with whom we already have FTAs—Singapore, Korea, Australia—already benefit, by virtue of MFN status, from some of the key enhancements negotiated in USMCA, that are absent in our existing bilateral FTAs. Thus, for example, these FTA partners currently enjoy the benefits of strong data flow and data localization rules (including for financial services) that the United States does not enjoy in their markets.[1]

DIGITAL TRADE RECOMMENDATIONS[2]

- ***Enable cross-border data flows in digital services.***

U.S. trade policy should further enable digital trade and the U.S. should be ambitious in its negotiations with respect to data flows and localization barriers. Cross-border data flows are critical to digital trade, and forced localization mandates make it difficult for U.S. exporters to expand into new markets. Analysis from the OECD has revealed an increasing level of restrictiveness for digitally-enabled services in part due to restrictions on cross-border movement of data.[3] Cross-border data flows are the lifeblood of global digital trade and by extension the array of industries that increasingly rely on the Internet to compete in the global marketplace. In the U.S., the productivity gains and efficiencies enabled by data flows have boosted the economy by hundreds of billions of dollars.

With an uptick in data-related barriers in recent years, trade discussions and clear rules are critical to ensure that any restrictions on the transfer, storage, and processing of data are targeted in a manner that does not unreasonably limit legitimate cross-border trade. Policies that restrict data flows, either directly through explicit data and infrastructure localization requirements, or indirectly for national security or other purposes, negate the productivity gains and efficiencies enabled by Internet

---

[1] If these countries were to take on similar binding commitments in an FTA with another country, we would equally enjoy rights in their market under MFN, but no country has replicated USMCA standards in full.

[2] These Recommendations reflect more extensive recommendations CCIA has filed with the Office of the U.S. Trade Representative and Department of Commerce in ongoing trade discussions such as IPEF, available at *https://www.ccianet.org/2022/04/ccia-offers-recommendations-for-u-s-policymakers-on-indo-pacific-economic-framework/*.

[3] OECD Services Trade Restrictiveness Index: Policy Trends up to 2020, available at *https://issuu.com/oecd.publishing/docs/oecd-stri-policy-trends-up-to-2020?fr=sNmVlNzYxOTI3Mw*.

platforms and cloud computing while often simultaneously undermining digital security globally.

The U.S. should continue to pursue rules that prohibit governments from interfering with data flows or the exchange of information online, and prohibit regulations or standards that condition market access, procurement, or qualification for widely-used certifications based on nationality of ownership, location of corporate headquarters, or size of company.

Specifically, rules should prohibit governments from imposing data localization or local presence requirements on data controllers or processors, as well as linking market access and/or commercial benefits to investment in or use of local infrastructure. Often, such policies not only restrict foreign market access and investment, they become counter-productive as they hinder services providers' ability to diversify and backup data, instead centralizing it all in one or a handful of local data centers. These rules should also extend to financial services. To the extent possible, these prohibitions should apply to both explicit and indirect measures such as ill-fitting privacy and cybersecurity measures, industrial policy, and censorship disguised as national security protections to keep data in a particular country.

CCIA cautions strongly against introducing new exceptions to trade rules applicable to localization and cross-border data flows as a response to claims that trade rules constraint domestic regulatory from activating in the public interest. While requirements over how data is stored, processed, and transmitted may well evolve over time, the existing rules do not constrain such evolution. In the rare cases where localization can be justified, existing exceptions provide broad scope for addressing legitimate policy concerns.

- ***Foster trust in digital services and growth of new technologies.***

Trust is fundamental to the growth and cross-border delivery of these services. Without adequate privacy protections and security in digital communications, governments may continue to enact restrictions on cross-border services citing perceived risks. Privacy and consumer protections and trade rules should work in tandem to further the goals of initiatives promoting trustworthy data flows. To that end, trade agreements should encourage the development of national privacy legislation that sets clear rules on the use of personal data domestically, promote the adoption of bilateral and multilateral agreements on government access to data such as those being pursued by the OECD,[4] and commit to codify protections for valid basis for transfer of personal data such as the APEC Cross-Border Privacy Rules into domestic law.

With respect to artificial intelligence (AI), trade agreements should encourage the adoption and deployment of trustworthy AI technologies by referencing principles and agreements that reflect multi-stakeholder input such the OECD Council Recommendations on Principles for responsible stewardship of trustworthy AI or the goals referenced in the White House's AI Bill of Rights.

- ***Prohibit customs duties for electronic commerce.***

Imposing customs requirements on purely digital transactions creates significant and unnecessary compliance burdens on nearly all enterprises, including small and medium-sized enterprises (SMEs). The moratorium on imposing customs duties for electronic transmissions has been key to the development of global digital trade and shows the international consensus with respect to the digital economy. The moratorium was most recently renewed at the 12th WTO Ministerial Conference in June 2022, and the commitment not to impose duties on electronic transmissions is reflected in the number of commitments made in free trade agreements among multiple leading digital economies. Permanent bans on the imposition of customs duties on electronic transmissions are a frequent item in trade agreements around the world and have been part of all U.S. FTAs for the past two decades.

The United States should continue to embed in trade agreements commitments resulting in a permanent ban on the imposition of customs duties on electronic transmissions. Enshrining the moratorium in agreements would enhance bilateral trade while also continuing to discourage other countries from including electronic transmission in their domestic tariff codes, as one IPEC member, Indonesia, has already sought to do.

---

[4] *See https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm; https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.*

- ***Prohibit unilateral and discriminatory taxes.***

International trade requires a consistent and predictable international tax system, and tax measures play a significant role in the global competitiveness of U.S. companies. Any country that the United States seeks a trade agreement with should not impose digital taxation measures that are discriminatory in nature and contravene long-standing principles of international taxation, and the U.S. should seek to include commitments not to pursue unilateral and discriminatory digital taxation measures in forthcoming trade and economic pacts.

- ***Address state-censorship practices and combat rising digital authoritarianism.***

Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets, including those of major trading partners, and even in some larger developed markets and is accomplished through different tools and methods.[5]

Allied governments have a critical role to play in partnering with technology companies and leading in the defense of Internet freedom and open digital trade principles. Government-imposed restrictions of digital services and online content can take multiple forms, and the risks associated with each method or regulatory framework providing for censorship methods can vary greatly.

The U.S. should work with trading partners to address rising digital authoritarianism and state-censorship practices that pose threats to the open Internet and freedom of expression around the world. Countries should affirm commitments under Article 19 of the International Covenant on Civil and Political Rights as they apply to defending free expression online. Making Article 19 binding and enforceable under a trade agreement would significantly enhance the value of this commitment. Parties should pursue commitments to refrain from blocking or restricting access to lawful online content, digital services, and infrastructure underlying Internet delivery. This is consistent with the goals of the U.S.-led Declaration for the Future of the Internet that encourages like-minded countries to promote fundamental freedoms online and combat actions by authoritarian governments. The United States should look to embed similar commitments to ensure an open Internet in trade disciplines as well.

- ***Secure digital communications and devices and prevent bans on encryption.***

Providers of digital devices and services continue to improve the security of their platforms through the deployment of technologies that safeguard the communications and commercial transactions that they enable. Strong encryption has been increasingly enabled on now-ubiquitous smartphones and deployed end-to-end on consumer-grade communications services and browsers. Encrypted devices and connections protect users' sensitive personal and financial information from bad actors who might attempt to exploit that information.

Many countries, at the behest of their respective national security and law enforcement authorities, have passed laws that mandate access to encrypted communications. Often the relevant provisions are not explicit, but mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders. Other versions require access to or transfer of source code related to encryption as a condition of allowing technology imports. Such exceptional access regimes run contrary to the consensus assessments of security technologists because these rules are technically and economically infeasible to develop and implement. Companies already operating in countries that have or are considering anti-encryption or source code access laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption or facilitated access requirements to be barriers to entry.

The United States should continue efforts to promote regulatory cooperation and international standards and best practices for securing products and services. Trade agreements should contain commitments to promote encrypted devices and connec-

[5] The U.S. International Trade Commission released its report on foreign censorship policies in January 2022 and detailed how extensive these practices have become. U.S. International Trade Commission, Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses (February 2022), available at *https://www.usitc.gov/publications/332/pub5244.pdf* at 21.

tions, and adherence to frameworks such as the NIST-developed Cybersecurity Framework. Specifically, the agreement should prevent countries from compelling manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm specification, or other cryptographic design details. Similarly, the agreement should prohibit governments from conditioning market access, with appropriate exceptions, on their ability to demand access to cryptographic keys or source code.

Additionally, the agreement should include commitments for partners to pursue risk-based cybersecurity measures, and utilization of open, consensus-based international standards as they are the more effective approach in comparison to prescriptive regulation. Trading partners should pursue cooperative approaches to cybersecurity and incident responses, including sharing of information and best practices with respect to vulnerability disclosure.

- ***Foster innovation in artificial intelligence.***

Emerging technologies such as artificial intelligence (AI) and machine learning, as well as quantum computing, increasingly impact cross-border trade, and trade rules increasingly govern the development and growth of these technologies. The United States should ensure regulatory practices and technical standards are in alignment to foster open lines of cooperation. To continue to use and export AI and other emerging technologies, businesses and users need a trade framework that allows them to move data and infrastructure safely across borders while ensuring that other countries will not misuse legal systems to impede the growth of new technologies. This will enable use of emerging technologies in addressing global challenges such as public health, humanitarian assistance, and disaster response. Work on promoting AI alignment and export competitiveness should not clash or otherwise undermine existing efforts such as the ongoing National Institute of Standards and Technology AI Risk Management Framework process aimed at implementing a risk-based and flexible AI regulatory landscape.

Trade rules that can facilitate the responsible cross-border growth of AI technologies include those that enable cross-border data flows and remove localization requirements; encourage governmental investment in and release of open data; identify and share best practices for the responsible use of AI; engage in cooperation and public-private collaboration on AI; and adopt innovation-oriented copyright rules that enable machine analysis of data. In addition, to ensure substantive convergence and avoid the potential for discriminatory outcomes, the U.S. and its trading partners should agree to avoid adopting any measures that discriminate against U.S. suppliers who excel in this area by providing less favorable treatment to AI products or applications than they give to like products or applications without an AI component.

As a matter of good regulatory practice, the development and implementation of AI regulations should include: adopting a risk-based approach, including transparent processes for assessing, managing, and mitigating risks associated with specific AI applications; assessing whether potential risks can be mitigated or addressed using existing instruments and regulatory frameworks; considering whether any new or proposed regulation is proportionate in balancing potential harms with economic and social benefits; employing risk management best practices, including considering the risk-substitution impact of a specific AI application against a scenario where that application has not been deployed but baseline risks remain in place; and promoting the development of voluntary consensus standards to manage risks associated with AI applications in a manner that is adaptable to the demands of dynamic and evolving technologies.

In addition to trade rules, countries should work together to facilitate research and development of new applications of AI to address shared challenges; facilitate dialogues among all stakeholders including governments, civil society, academia, and the private sector on best regulatory practices; and pursue joint discussions on the responsible and ethical use of AI.

- ***Promote global practices on Internet access and interconnection policies.***

The United States should work to protect the interoperable and interconnected nature of the global Internet architecture that enables cross-border data flows, support principles of non-discrimination and market access to telecommunications networks, and enable stakeholders to negotiate the nature of services to be delivered across the network on a voluntary market-driven basis, based on reasonable business practices agreed upon by both sides.

Globally, the business practice on Internet interconnection is for content and application providers and ISPs to enter into agreements through autonomous negotiations. To protect the Internet ecosystem, the growth of the tech industry globally, and ensure these investments can continue to flourish and support digital trade, the United States should seek to include assurances that Internet-based telecommunications service providers seeking the exchange of traffic with content and application providers, and vice versa, are able to negotiate with the other party on a voluntary, market-driven basis in this agreement. Trade rules should prevent new mandates to negotiate with ISPs, and the unilateral imposition of fees, as a condition for reaching end-user customers. This builds on existing trade rules that ensure that access to domestic telecommunications networks is facilitated on reasonable and non-discriminatory terms.

- ***Commit to following good regulatory practices.***

The global Internet economy is at a pivotal moment in its development. Countries are moving quickly to introduce new, at times experimental, regulatory frameworks for digital services, and seek to craft rules on the development of emerging technologies with the aim to ensure that the digital economy remains a tool for openness and free exchange that has led to unprecedented growth and opportunity.

As new proposals are introduced around the world, countries should commit to following good regulatory practice and work together to ensure that regulations do not have unintended impacts. International regulatory cooperation is an important tool for improving regulatory quality, reducing the likelihood of creating trade barriers or unnecessary regulatory differences, aligning regulation with shared principles and values, avoiding unintended consequences or conflicts with broader foreign policy objectives, building trust and expertise among regulators, and deepening understanding of trends in regulatory governance to inform current and future approaches to policymaking. As new regulations take effect in foreign markets, it will be essential that the U.S. work with trading partners to ensure that implementing regulations are fair, implemented in a non-discriminatory manner against foreign firms, and are subject to adequate oversight and due process.

The United States should pursue governing principles of the digital economy that ensure that regulations should be non-discriminatory and principles-based, made pursuant to a transparent regulatory process, ensure due process to those affected, and include adequate safeguards to reduce the impact of any unintended consequences.

- ***Address technical barriers to trade.***

U.S. technology exporters face a growing number of non-tariff measures such as technical regulations, conformity assessment practices, and standards-based measures. Adoption of global standards is critical to ensuring regulatory coherence and avoiding country-specific standards that deter market entry. Some U.S. cloud service providers (CSPs) have been unable to serve the public sector due to onerous security certification requirements that deviate from internationally accepted standards and make it impossible for CSPs to comply without creating a market-unique product, including physically segregating facilities for exclusive use for government-owned customers and onshoring of data. The adoption of country-specific standards creates de facto trade barriers for U.S. companies and raises the costs of cutting-edge technologies for consumers and enterprises.

The United States should (1) pursue commitments like those outlined in USMCA Chapter 11 on addressing technical barriers to trade; and (2) pursue commitments to follow good regulatory practices of these commitments in the development of standards, regulations, and conformity assessment procedures for services.

- ***Enable trade in electronic payment services.***

Electronic payment (e-payment) systems which are interoperable across borders are critical in enabling the growth of cross-border digital trade. Trade policy can help drive the development of cross-border e-payment systems through commitments on the free flow of data including financial services data, promoting interoperability through international standards, and encouraging open innovation and competition through the adoption of open e-payment models such as real-time payments (RTP) systems and encouraging open application programming interfaces (APIs) to allow all e-payment service providers to compete. Additionally, the United States should pursue provisions on electronic signature, electronic authentication, paperless trading, and other best practices often included in trade agreements.

- ***Promote copyright frameworks that enable emerging technologies and digital services.***

As part of U.S. trade policy, the U.S. should promote intellectual property frameworks that reflect U.S. law and secure commitments that will foster innovation in emerging technologies. This is reflected in a few areas of copyright traditionally included in trade agreements.

First, a flexible copyright regime is necessary for the continued growth of the digital economy. Principles such as fair use are a cornerstone of U.S. copyright law and industries that rely on this right are a significant contributor to the U.S. economy and exports. Fair use is also critical to activities central to new areas of innovation and cutting-edge technology such as artificial intelligence and text and data mining. Additionally, mandated technological protection measures (TPMs) are a frequent inclusion in U.S. trade agreements. Corresponding statutory exceptions to these anti-circumvention measures are a critical component of these provisions. Consistent with USMCA, any TPM provision should include exceptions to anti-circumvention that are consistent with 17 U.S.C. § 1201, including § 1201(f) on reverse engineering and interoperability, in providing limitations and exceptions to TPMs.

Intermediary liability protections for Internet service providers, such as the framework in Section 512 of the Digital Millennium Copyright Act in the United States, have been critical to growing the U.S. digital economy by providing business certainty to U.S. investors and innovators. U.S. trade policy has long reflected domestic copyright principles by including necessary intermediary protections for online services in trade agreements dating back to 2003. USMCA continues this tradition, drawing directly upon Title 17 of the U.S. Code.

E-MERCHANTS TRADE COUNCIL, INC.
1655 North Fort Myer Drive, Suite 700
Arlington, VA 22209
(703) 574–0000
https://www.emtc.org/

On behalf of the E-Merchants Trade Council, Inc. (EMTC), I am Marianne Rowden, CEO of EMTC and respectfully submit this statement for the record. EMTC appreciates the opportunity to comment concerning the topics covered in the hearing on "Opportunities and Challenges for Trade Policy in the Digital Economy" held on November 30, 2022.

EMTC was formed in July 2021 to represent the interests of the e-commerce industry by creating a global community of micro, small and medium size enterprise (MSMEs) e-sellers, marketplace platforms, and service providers to resolve trade, tax and transportation challenges. EMTC's advocacy mission is to support national and international policies that simplify cross-border transactions of physical and digital goods. EMTC facilitates dialogue among the E-Merchant worldwide community and global regulators.

EMTC applauds the Subcommittee for holding this hearing on "Opportunities and Challenges for Trade Policy in the Digital Economy." We recommend that the Subcommittee hold more hearings, roundtable discussions, and town hall meetings throughout the United States to receive testimony, comments and input from as many stakeholders as possible since the United States' trade policy on digital trade affects every segment of American society. EMTC's comments address the three (3) issues posed to the witnesses during the hearing.

1. What is Digital Trade?

As noted in the introductory paragraph describing EMTC, we use the nomenclature of "digital trade" to describe "digital goods" or electronic articles such as software, images, music, games etc. that are non-physical and transmitted via the Internet by e-mail, the cloud, etc.[1] EMTC makes this distinction for cross-border transactions

[1] We note that the World Trade Organization (WTO) has defined "electronic commerce" as "the production, distribution, marketing, sale or delivery of goods and services by electronic means." *See* Work Programme on Electronic Commerce (Adopted by the General Council on September 25, 1998) at: *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/274.pdf &Open=True.* The World Customs Organization (WCO) defines "cross-border e-commerce" as "all transactions which are effected digitally through a computer network (*e.g.,* the Internet) and result in physical goods flow subject to Customs formalities." *See* WCO Framework of Standards on Cross-Border E-Commerce Definitions at: *https://www.wcoomd.org/-/media/wco/public/*

Continued

due to the long-standing general rule under Treasury Decision 85–124 that software is classified under heading 8523 of the Harmonized Tariff Schedule of the United States (HTSUS) but the duty is based on the declared value of the carrier medium (*e.g.,* CD–ROM, USB drive, floppy disk, magnetic tape). EMTC also views "digital trade" to encompass all the rules governing data (*e.g.,* privacy, localization, etc.).

Traditionally, customs regimes regulated physical goods for assessing customs duties. Since adopting the Declaration on Global Electronic Commerce in 1998, the WTO members agreed to a moratorium on customs duties on electronic transmissions, which has been revisited and extended by the WTO every two years at its ministerial conference.[2] In 2021, India and South Africa put forward a communication on The Moratorium on Customs Duties on Electronic Transmissions: Need for Clarity on its Scope and Impact.[3] We note that the moratorium applies to the "transmission" and not the assessing of customs duties on the content of the transmission (*e.g.,* the value of the software, music, image, etc.).

We echo the hearing witnesses' concern that the Moratorium is set to expire by the next WTO Ministerial Conference (scheduled for December 2023) or March 31, 2024, if the ministerial is delayed.[4] EMTC's policy preference is for the United States to lead the effort to make the moratorium permanent. However, EMTC is alarmed that there are no discussions in any country about how customs administrations will implement the mechanisms to assess and collect customs duties on digital transmissions and to subject digital goods to the same regulatory requirements as physical goods.

2. Why is Digital Trade Important?

EMTC believes it is critical for Congress to set United States digital trade policy because of the convergence between digital and physical goods as a result of the state of flux in the WTO e-commerce negotiations. Moreover, digital trade comprises an increasing percentage of global trade, particularly for the United States as a leader in digital goods and services.

We recommend that the Subcommittee create a framework that acknowledges the new entities engaged in cross-border trade for both e-commerce of physical goods (*e.g.,* foreign sellers, e-commerce marketplace platforms, fulfillment houses, logistics companies) and trade in digital goods. It is critical that the Subcommittee properly allocate regulatory responsibilities appropriate to the role of the entity in the transaction as there may be more or different intermediaries and agents involved in cross-border shipments rather than a single manufacturer/shippers, carrier, customs broker, and importer of record.

Moreover, it is important that any policy (and proposed statute) is neutral so that it does not disadvantage any company's business model, such as imposing the same regulatory requirements on marketplaces regardless of whether they provide logistics services handling the goods versus offering a means of a sales transaction. Likewise, EMTC urges the Subcommittee to be sensitive to the impact of regulatory requirements on small-medium size e-sellers as they are only able to engage in global trade through e-commerce and work on low profit margins due to competition and the numerous fees that marketplaces charge.

EMTC believes that future trade agreements, such as the Indo-Pacific Economic Framework (IPEF), should include specific chapters on Customs and Trade Facilitation similar to Chapter 7 of the United States Canada Mexico Agreement (USMCA) which emphasizes trade facilitation:

> Article 7.1: Trade Facilitation
>
> 1. The Parties affirm their rights and obligations under the Agreement on Trade Facilitation, set out in Annex 1A to the WTO Agreement.

---

global/pdf/topics/facilitation/activities-and-programmes/ecommerce/2_definitions_en.pdf?db=web.

[2] *See,* Declaration on Global Electronic Commerce (Adopted May 20, 1998) at *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q%3A%2FWT%2FMIN98%2FDEC2.pdf&Open=True.*

[3] *See,* The Moratorium on Customs Duties on Electronic Transmissions: Need for Clarity on its Scope and Impact (Adopted November 8, 2021) at: *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q%3A%2FWT%2FGC%2FW833.pdf&Open=True.*

[4] *See,* Work Programme on Electronic Commerce Draft Ministerial Decision of June 16, 2022 at: *https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q%3A%2FWT%2FMIN22%2FW23.pdf&Open=True.*

2. With a view to minimizing the costs incurred by traders through the importation, exportation, or transit of a good, each Party shall administer its customs procedures in a manner that facilitates the importation, exportation, or transit of a good, and supports compliance with its law.

3. The Parties shall discuss within the Trade Facilitation Committee established under Article 7.24 (Committee on Trade Facilitation) additional measures to facilitate trade. The Parties are encouraged to adopt additional measures that build on the obligations in this Chapter with a view to further facilitating trade.

See, USMCA Ch. 7 on Customs Administration and Trade Facilitation at *https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/07_Customs_Administration_and_Trade_Facilitation.pdf*. Often importers and exporters find themselves in the difficult situation of regulatory agencies interpretation of a free trade agreement which eviscerates the spirit of free trade in order to meet regulatory compliance requirements. Therefore, negotiators should prioritize "minimizing the costs incurred by traders" and facilitate trade.

a. Increase *De Minimis*

As a preliminary point, we note that e-commerce is not the same as *de minimis* and *vice versa*—that is, not all e-commerce shipments are entered as low-value shipments under 19 U.S.C. § 1321 and not all *de minimis* shipments were ordered online. For EMTC's members who are service providers (*e.g.,* customs brokers, logistics companies, etc.), whether an article is ordered online makes no difference to its handling in a cross-border transaction.

EMTC strongly believes that the United States should prioritize getting other countries to increase their *de minimis* threshold for low-value shipments. This will go a long way to increase MSME participation in global trade, especially for U.S. e-seller exporters. Most other countries have a *de minimis* level between $0 and $200 whereas the United States *de minimis* threshold is $800. The United States was successful in getting Canada and Mexico to increase those countries' *de minimis* in the USMCA.

Title 19 U.S.C. § 1321 on Administrative Exemptions has been part of the customs statute since the Tariff Act of 1930. Specifically, the *de minimis* threshold under 19 U.S.C. § 1321(a)(2)(C) for articles free of duty "in any other case" was initially set at $1 and periodically raised by Congress—first, to $5 in 1978, and $200 in 1993 as part of the Customs Modernization Act, Title IV of NAFTA.[5] Congress increased the *de minimis* to $800 recently in the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. 114–125, 130 Stat. 223. As these amendments demonstrate, Congress has raised the *de minimis* every few decades taking into account the erosion of purchasing power as a result of inflation. EMTC believes this level for *de minimis* is appropriate given reports of inflation at over 6% for 2021 and in excess of 7.5% year-to-date. Congress should commit support for the current U.S. *de minimis* level and stress for near reciprocity in treatment of low-value shipments in the Indo-Pacific countries within a limited phased implementation period.

EMTC is aware of the possibility of Congress revisiting *de minimis* and lowering the threshold under 19 U.S.C. § 1321(a)(2)(C) in the America COMPETES Act (Import Security and Fairness Act),[6] but we believe that such policy instability makes it very difficult for companies to plan when they have organized their business operations based on the $800 threshold level. It is precisely because Congress has only increased the *de minimis* threshold infrequently every few decades that makes the possibility of a change after only six (6) years from passage of TFTEA in 2016 greatly concerning to the trade community, particularly e-commerce marketplace platforms, e-sellers and companies that provide trade and transportation services to e-commerce companies.

Since the passage of TFTEA in 2016, the trade community faced the prospect of lowering the *de minimis* threshold under 19 U.S.C. § 1321(a)(2)(C) twice. First, during the negotiation of the USMCA in 2019, the Administration negotiated to raise the *de minimis* threshold for imports to Mexico (to $117) and Canada (to $150), but included a footnote:

---

[5] *See,* list of legislative amendments for 19 U.S.C. § 1321 at *https://uscode.house.gov/view.xhtml?path=/prelim@title19/chapter4&edition=prelim.*

[6] *See,* Import Security and Fairness Act, H.R. 6412, 117th Congress (2022).

> Notwithstanding the amounts set out under this subparagraph, a Party may impose a reciprocal amount that is lower for shipments from another Party if the amount provided for under that other Party's law is lower than that of the Party.

USMCA Ch. 7 Customs Administration and Trade Facilitation, Article 7.8.1(f) Express Shipments, footnote 3 at 7–7.[7] As a result of the trade community's advocacy efforts, Congress wrote a letter to the U.S. Trade Representative (USTR) stating:

> We strongly oppose any effort by the Executive Branch to lower the current $800 *de minimis* threshold through USMCA implementing bill, including any amendment to 19 U.S.C. 1321 that would grant the Executive Branch additional authority to decrease or eliminate the threshold.
>
> The U.S. *de minimis* threshold is a policy recently set by Congress, which raised the threshold from $200 in 2016. The current *de minimis* threshold still enjoys wide bipartisan support in Congress and throughout the manufacturing, retail, logistics, and e-commerce landscapes. In our view, it is neither necessary, appropriate, nor desirable to change this policy in U.S. law as part of the implementation of USMCA's requirements. In fact, we consider that such an effort would amount to an override of Congressional authority by the Executive Branch, and thus would be entirely inappropriate.

Letter from the Congress of the United States to Ambassador Robert E. Lighthizer, U.S. Trade Representative dated October 18, 2019.[8] EMTC believes that the better policy from a U.S. leadership position is to get other countries to raise their *de minimis* threshold, as the U.S. accomplished in the USMCA, rather than to lower the U.S. *de minimis*.

3. How Can the U.S. Work with its Allies?

EMTC is concerned that there are numerous allies, particularly its largest trading partners (*e.g.,* the European Union) where trade policy is diverging, including:

a. Small-medium e-sellers' compliance with the U.S. 1099K income reporting at $600 requirement;
b. Updating import and export data for low-value shipments;
c. Algorithmic decision-making for compliance and risk management;[9]
d. U.S. implementation of the OECD tax treaty (Pillar II) and the UN vote on global tax standards;
e. The EU's Carbon Border Adjustment Mechanism;
f. Changes to *de minimis* and Value Added Tax rates for low-value shipments; and
g. The different approaches of the EU and the U.S. on regulating the digital economy (*e.g.,* the EU's Digital Markets Act and Digital Services Act).

Our observation is that the European Union has chosen to create a new body of law to regulate the digital economy whereas the United States seems to be integrating digital provisions into existing titles of federal statute. As a result, the process of aligning policies with our trading partners may be a challenge.

4. Conclusion

In summary, EMTC believes that the Subcommittee should carefully consider creating a trade policy which creates a framework to integrate equal treatment of physical and digital goods, accommodate new entities in the global trade ecosystem, and does not create regulatory burdens on MSME e-sellers, such as lowering the *de minimis* under 19 U.S.C. § 1321(a)(2)(C).

EMTC appreciates the opportunity to comment on the testimony presented at the hearing on Opportunities and Challenges for Trade Policy in the Digital Economy, and we are happy to discuss the ideas expressed above in more detail.

---

[7] *See, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/07_Customs_Administration_and_Trade_Facilitation.pdf.*

[8] *See* letter at: *https://schweikert.house.gov/2019/01/10/congressman-david-schweikert-leads-letter-representative-lighthizer/.*

[9] The European Parliamentary Research Service has produced a study in March 2019 on "Understanding Algorithmic Decision Making: Opportunities and Challenges" and a number of factors mentioned come from this report (applied in a customs context), which can be found at: *https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.* The United States' National Institute of Standards and Technology has released its "AI Risk Management Framework: Second Draft" at: *https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.*

ENGINE ADVOCACY
700 Pennsylvania Ave, SE
Washington, DC 20003

December 7, 2022

U.S. Senate
Committee on Finance
Subcommittee on International Trade, Customs, and Global Competitiveness
Dirksen Senate Office Bldg., Rm. SD–219
Washington, DC 20510–6200

Dear Chairman Carper, Ranking Member Cornyn, and honorable members of the subcommittee on International Trade, Customs, and Global Competitiveness:

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. Accordingly, we appreciate the committee holding a hearing on the Opportunities and Challenges for Trade Policy in the Digital Economy.

The Internet and digitization of world economies has enabled startups to reach markets beyond their borders. Through digital trade, startups are able to further the outsized contributions they make to domestic economic growth and job creation. And startups help others reach markets abroad too, whether they be artists, farmers, manufacturers, or others. As digital trade has grown,[1] barriers to digital trade have grown along with it. Startups encounter these barriers as they grow and scale beyond U.S. borders to serve users and clients abroad, and such barriers dictate where startups can feasibly reach users.[2]

Digital trade policies that lower trade barriers for U.S. businesses face criticism from policymakers[3] and others[4] that claim that forward-thinking digital trade policies only serve large incumbent companies. Reducing barriers to digital trade helps all U.S. businesses, including "big tech," but it arguably stands to help startups the most. Take, for instance, the invalidation of Privacy Shield in 2020 created barriers to cross-border data transfers between the U.S. and Europe. This impacted all transatlantic businesses, but large companies were able to turn to other methods for transferring data, like Standard Contractual Clauses, while startups faced more existential business disruptions, increased costs, and lost clients.[5] Indeed, small businesses and startups comprised the overwhelming majority of companies that relied on free flows of data through Privacy Shield.[6] Similarly, the EU's Digital Services Act will impact all content-hosting companies operating or looking to operate in Europe. Large U.S. technology companies will face significant new obligations under the law, but none of them are likely to exit the EU market or significantly revise plans to operate there. U.S. startups on the other hand will encounter elevated barriers to entering the EU market, significant new obligations, and compliance costs.[7] U.S. policymakers have intervened in both of these cases to try to reach

---

[1] *See e.g.,* Table 3.1. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service, Bureau of Economic Analysis (July 7, 2022), *https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4#reqid=62&step=9&isuri=1&6210=4.*

[2] *See e.g.,* Comments of Engine Advocacy Regarding Foreign Trade Barriers to U.S. Exports for 2023 Reporting, Engine (October 28, 2022), *https://engine.is/s/2022-Transatlantic-Business-Statement-on-EU-US-Data-Privacy-Framework.pdf.*

[3] *See e.g.,* Hearing on Opportunities and Challenges for Trade Policy in the Digital Economy: Hearing Before the Subcommittee on International Trade, Customs, and Global Competitiveness, 117th Congress (2022) (remarks of Senator Warren).

[4] *E.g.,* "Digital Trade" Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies, Rethink Trade (November 2, 2022), *https://rethinktrade.org/reports/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/.*

[5] *See e.g.,* Sean Davis, New Transatlantic Data Deal Can Reopen EU Opportunities for Startups, Engine (April 20, 2022), *https://engineadvocacyfoundation.medium.com/new-transatlantic-data-deal-can-reopen-eu-opportunities-for-startups-4a25e454572f;* #StartupsEverywhere profile: Mikel Carmenes Cavia, Co-Founder and VP of Engineering, Onfleet, Engine (May 7, 2021), *https://www.engine.is/news/startupseverywhere-sanfrancisco-ca-onfleet.*

[6] *See generally,* Privacy Shield Participants, *https://www.privacyshield.gov/list.*

[7] Lauren Koop, The EU's Digital Services Act is one step closer to becoming law. How will it impact U.S. startups?, Engine (July 28, 2022), *https://engineadvocacyfoundation.medium.*

Continued

solutions with their EU counterparts.[8] This work advances the interests of U.S. startups, and should not be foregone merely because it also helps or is supported by "big tech."

Smart digital trade policy that promotes a free, open, and global Internet is needed to lower and keep low barriers to trade for startups. The recent U.S.-Mexico-Canada and U.S.-Japan Agreements enshrined commonsense digital frameworks and can provide a template for smart digital trade policy and future trade agreements. Inspired by these agreements, digital trade policy should embrace the following principles, which can support the success of U.S. startups looking to expand into foreign markets and engage customers abroad:

Provide proportionate, tailored, and certain intermediary liability frameworks.
Balanced intermediary liability frameworks, like those found in the U.S., provide the legal certainty needed for startups with business models that rely on user content—whether it's comments, photos, reviews, etc.—to grow and thrive. Around the world, however, common methods for governing intermediaries are taking root that undermine a startup-friendly environment and create new uncertainties and costs for U.S. companies. Laws that require the appointment of local representatives, impose tight content takedown timelines, require automated filtering, require the removal of content that is not otherwise illegal, and threaten heavy fines create barriers to entry for startups and reduce the number of foreign markets available to them.

Facilitate cross-border data flows.
The Internet allows startups to access foreign markets with little additional investment. Conversely, policies that restrict how and when data can be transferred across borders erect barriers to trade and increase costs that startups with limited resources have difficulty overcoming compared to their larger rivals.

Foster innovation and market access.
Extraterritorial regulations adopted in other jurisdictions, including around data privacy and emerging technologies, can limit innovation opportunities and market access for American startups. Because they often apply any time a business encounters a user in or from that jurisdiction, startups with relatively few users there are likely to forgo serving that jurisdiction because of the regulatory structure. U.S. policymakers should work through the appropriate fora to ensure American startups encounter a consistent and level playing field.

Avoid technology sector-specific levies.
While startups are rarely subject to digital services taxes (DSTs) themselves, they rely on the services of larger companies who are, to build their products and reach customers. DSTs increase the price of these services, putting startups at a disadvantage in jurisdictions with them. Working through multinational fora to reach a global solution promises the best step toward a uniform tax environment.

Prohibit duties on digital transactions.
The WTO moratorium on e-commerce is critical to fostering digital trade, and it is especially important for startups. Since 1998, member countries have

---

com/the-eus-digital-services-act-is-one-step-closer-to-becoming-law-how-will-it-impact-u-s-startups-7be702180582; Daphne Keller, The EU's new Digital Services Act and the Rest of the World, Verfassungsblog (November 7, 2022), *https://verfassungsblog.de/dsa-rest-of-world/* (Explaining the comparative impacts of the DSA on small entities: "The other predictable global harm will be to competition. The DSA burdens even very small platforms with obligations that today's incumbents never shouldered, or else took on only much later in their development. Facebook, for example, first released a transparency report in 2013, when it was worth $139 billion. It first allowed users to appeal removals of photos, videos, and posts (but not comments) in 2018, when the company was worth $374 billion and had some 35,000 employees. Newer market entrants will take on similar obligations at a much earlier stage: once they reach just €10 million and 50 employees.").

[8] *See, e.g.,* FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, White House (October 7, 2022), *https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/* (on resolving transatlantic data transfer issues); Chamber of Progress (@ProgressChamber), Twitter (December 8, 2021), (Remarks of Sec. Raimondo on the DSA: "We have serious concerns that these proposals will disproportionately impact U.S.-based tech firms and their ability to adequately serve EU customers and uphold security and privacy standards.").

agreed to not impose customs duties on electronic transmissions, but some countries have recently expressed interest in limiting or ending the moratorium.

In addition to these principles, there are other affirmative steps that U.S. policymakers can and should take to support startups and small businesses as they look to trade internationally. Witnesses highlighted several examples in response to questioning from Chairman Carper regarding such positive steps available.[9] Improved commercial guides and other trade resources from the Commerce Department would be helpful for startups. Startups turn to these and other government trading resources, but often find them insufficient.[10] Helping to increase the adoption of digital tools for small businesses could also help startups while expanding trade. Technology startups often already make use of digital tools to run their businesses and facilitate international trade, but since many startups offer digital services themselves, incenting increased adoption of such tools will help expand markets for startups. Finally, most government trade resources available for small businesses are focused toward exporters of physical goods. Many technology startups export software or services digitally, and would benefit from these government resources, like commercial guides, consulting services, and grant assistance,[11] being expanded to more directly support them.

Engine appreciates the opportunity to submit this statement for the hearing record and the Committee's attention to digital trade issues important to startups. We look forward to being a resource for the committee on these and other issues in the future.

Sincerely,

Engine Advocacy

PEN AMERICA
1100 13th Street, NW, Suite 800
Washington, DC 20005

PEN America stands at the intersection of literature and human rights to protect free expression in the United States and around the globe. Our PEN Charter calls us to uphold "the principle of unhampered transmission of thought within each nation and between all nations." We champion the freedom to write and work to unite writers and their allies to celebrate creative expression and defend the liberties that make it possible. It is under these principles that we see coerced censorship as a key barrier to trade in the digital economy.

PEN America defines "coerced censorship" as *the direct or indirect governmental suppression of digital content, in whole or in part, due to its perceived political or societal offense, consistent with international law, with special attention to Article 19 of the International Covenant on Civil and Political Rights. The term shall not be construed to include government actions related to data privacy, antitrust enforcement, or anti-harassment orders.* This definition seeks to precisely target efforts against extraterritorial censorship, while allowing for commonsense regulation of technology companies by our democratic allies.

As the long arm of authoritarianism grows, freedom of expression is stifled in every part of the world. Beijing's efforts are especially worrying due to its economic reach and marked intolerance of dissent. Censorship can be both overt and behind-the-scenes, with Chinese government influence creeping into LinkedIn profiles,[1] Zoom

---

[9] *E.g.,* Hearing on Opportunities and Challenges for Trade Policy in the Digital Economy: Hearing Before the Subcommittee on International Trade, Customs, and Global Competitiveness, 117th Congress (2022) (remarks of Christine Bliss).

[10] *See e.g.,* #StartupsEverywhere Profile: Jeff Wigh, Founder and CEO, Bryght Labs, Engine (February 4, 2022), *https://www.engine.is/news/startupseverywhere-overlandpark-ks-bryghtlabs* (remarking about some resources available via *Trade.gov,* how they apply to startups like his, and how they might be improved).

[11] *E.g.,* the State Trade Expansion Program (STEP), *https://www.sba.gov/funding-programs/grants/state-trade-expansion-program-step* (STEP needs to be reauthorized for FY 2023–26).

[1] *https://pen.org/press-release/pen-america-decries-linkedins-apparent-state-influenced-censorship/.*

meetings,[2] streaming services,[3] institutions of higher education,[4] and publishing houses.[5]

As PEN America documented in its landmark report Made in Hollywood, Censored by Beijing,[6] even one of our country's most iconic cultural industries increasingly self-censors in response to pressure, either direct or indirect, from the Chinese Communist Party. Increasingly, Beijing's economic clout has allowed it to insist that others comply with its censorship restrictions as a prerequisite to doing business with or in the country. These attempts to silence critical voices and stories must not go unanswered and we urge the inclusion of coerced censorship, and its definition, when discussing and legislating trade.

If you have any questions please reach out to our Managing Director in Washington, Nadine Farid Johnson (nfjohnson@pen.org) and our Senior Manager for Legislative Affairs, Laura Schroeder (lschroeder@pen.org).

PILOT INC.
C/O NeueHouse
110 East 25th Street
New York, New York 10010

December 14, 2022

U.S. Senate
Committee on Finance
Subcommittee on International Trade, Customs, and Global Competitiveness
Dirksen Senate Office Bldg., Rm. SD–219
Washington, DC 20510–6200

Dear Chairman Carper, Ranking Member Cornyn, and honorable members of the subcommittee on International Trade, Customs, and Global Competitiveness:

PILOT is a New York City-based, Delaware-registered startup that provides tech-driven virtual group coaching programs to companies that are easy to implement, affordable, and get good results. We employ over 50 individuals throughout the U.S. that are passionate about helping to empower each employee to truly own their career and actively shape their experience at work and our product has won many awards including Top HR Product of the Year. We are proud to be one of a small handful of certified LGBTQ-owned businesses providing enterprise Software as a Service (SaaS). Our customers include some of the largest companies in the world and we serve their employees—our end users—on five continents. From day one, PILOT was built to be a global company with global aspirations. That is why we appreciate the committee's attention to issues of digital trade and global competitiveness that are important to startups like PILOT.

To help startups like PILOT be competitive abroad, policymakers must pursue digital trade policies that lower barriers to entry, facilitate cross-border transfers of data, and promote uniform regulatory environments across jurisdictions. Data localization policies and regulatory regimes—especially around data protection and privacy—that vary from jurisdiction to jurisdiction increase the costs of serving customers and their employees in locations with these policies.

Compliance costs are not insignificant, especially for startups. I founded PILOT using my life's savings and we have bootstrapped since then, growing the business through the revenue we generate—we have not taken outside investment.

PILOT cares deeply about our users and keeping their data protected, and we have made significant investments to that end. Even with this focus, we must devote our limited resources to understanding our obligations and responding appropriately, especially when we serve customers abroad. High compliance costs amount to a transaction cost—a tax on doing business—that elevates barriers to operating in certain markets, without, in our view, any real tangible benefit to end users or our customers. Confusing and complex regulatory structures benefit large businesses who have the expertise and resources to comply and can amortize those costs across a

---

[2] *https://pen.org/press-release/pen-america-condemns-shuttering-of-chinese-activists-zoom-account/*.
[3] *https://pen.org/press-release/pen-america-denounces-disneys-removal-of-simpsons-episode/*.
[4] *https://pen.org/censorship-free-speech-issues-china/*.
[5] *https://foreignpolicy.com/2021/10/26/chinese-censorship-enes-kanter-celtics-browder-is-going-global/*.
[6] *https://pen.org/report/made-in-hollywood-censored-by-beijing/*.

huge base of business, while penalizing small innovative firms like PILOT, depressing economic growth. These costs can amount to 10 percent or more of the value of a contract.

The opportunity costs of compliance are not one to one. The resources devoted toward compliance that does little productive for our business could instead go toward additional innovation and job creation if those costs were reduced through smart digital trade policy. Savings from rationalized compliance policies free up dollars I can invest back into the business that helps us grow, in areas like marketing, sales, and R&D. That means we create more high-quality jobs for Americans in communities across the country, and generate more tax revenue for governments—all while adhering to our thoughtful and industry best-practices around data privacy and IT security, protecting our customer's data and our reputation.

The regulatory environment and resulting compliance costs impact our competitiveness as a startup in multiple ways. Larger competitors are better positioned to absorb these compliance costs. Cumbersome regulatory environments also impact our prospective customers, who respond by reducing the amount of vendors they have. That means they often consolidate their supplier base to work with a few large companies and startups like us lose out on critical business opportunities. And finally as a result of regulations abroad, prospective customers in other countries may instead turn to a domestic competitor who can offer a lower price or appear to reduce regulatory risk.

Smart digital trade policy informed by the real-world experiences of startups like PILOT is critical to bolster the global competitiveness of U.S. startups. We appreciate the committee's attention to these issues and hope that our perspective will prove helpful as you work with your colleagues across government in forming U.S. trade policy for the digital economy. Rationalizing these policies is critical to "unlock" America's renowned startup ecosystem, further facilitating the deployment of software and services around the world.

Sincerely,

Ben Brooks
Founder and CEO

PUBLIC CITIZEN'S GLOBAL TRADE WATCH
215 Pennsylvania Ave., SE
Washington, DC 20003
https://www.citizen.org/
(202) 454–5107

Statement of Melinda St. Louis, Director

Introduction

Public Citizen welcomes the opportunity to provide a written statement for the record for the Subcommittee Hearing: Opportunities and Challenges for Trade Policy in the Digital Economy. Public Citizen is a nonprofit consumer advocacy organization with more than 500,000 members and supporters. A mission of our Global Trade Watch division is to ensure that in this era of globalization, a majority 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 as well as identifying the dangers of so-called "digital trade" rules with respect to efforts to regulate the tech industry around the globe.

Over the past 3 decades, the Internet has grown to encompass, or at least touch on, nearly all aspects of economic and social life around the world. During this time, 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.

Lax domestic and global regulation has allowed Big Tech to enjoy broad and unfettered freedom to design, implement, and exploit e-commerce and digital systems and technologies. While new digital technologies, products, and systems have brought important benefits to people across the planet, the lack of oversight and regulation has enabled Big Tech to invade people's privacy, design and deploy a system of mass

corporate surveillance, leverage its 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 are grappling with how best to regulate Big Tech to protect consumer privacy, to ensure adequate competition, and hold companies accountable for discriminatory practices. Yet, behind closed doors in international trade negotiations, such as the U.S.-Mexico-Canada Agreement (USMCA) and the Japan-U.S. digital agreement, Big Tech has pushed digital trade terms that limit governments' ability to regulate their business practices. Big Tech continues to insert its deregulatory agenda [1] in a patchwork of new Biden administration trade initiatives, including the Indo-Pacific Economic Framework (IPEF), U.S.-EU Trade and Technology Council (TTC), and the U.S.-Kenya Strategic Trade and Investment Partnership (STIP), as well as ongoing discussions in the World Trade Organization's (WTO) E-commerce "Joint Statement Initiative." They seek binding rules to:

- Limit the ability of governments to regulate where Big Tech firms send and store our 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;[2]
- 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 and tie U.S. policymakers' hands for future regulatory efforts. More than 50 national organizations representing labor, civil rights, consumer, and other constituencies oppose these harmful "digital trade" provisions.[3]

USTR Katherine Tai has articulated a more forward-thinking vision:

> Our approach to digital trade policy must be grounded in how it affects our people and our workers. We must remember that people and workers are wage earners, as well as consumers. They are more than page views, clicks, and subjects of surveillance. They are content creators, gig workers, innovators and inventors, and small business entrepreneurs. This means they have rights that must be protected—both by government policy and through arrangements with other governments.[4]

Congress should monitor ongoing trade negotiations to ensure that any "digital trade" talks advance this vision and do not replicate problematic provisions pushed by Big Tech that were included in the USMCA.[5] Trade agreement rules on digital trade should not shrink the policy space of U.S. regulators and the U.S. Congress.

Limiting Government Regulation of Data Flows

Big Tech demands for "free flow of data" refers to binding rules to limit the ability of governments to regulate where Big Tech firms send and store our data. That would mean high-tech giants like Amazon, Google, and Facebook would be free to transfer our data to any other country. People's every move on the Internet and via

---

[1] *See* 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, accessed December 13, 2022.

[2] Anna Edgerton, "Tech Liability Shield Has No Place in Trade Deals, Groups Say," Bloomberg Law, published May 27, 2021, accessed December 13, 2022.

[3] Trade Justice Education Fund, "53 Organizations Warn About Harmful Provisions in 'Digital Trade' Pacts," Press release, November 2, 2021.

[4] Amb. Tai, "Remarks of Ambassador Katherine Tai on Digital Trade at the Georgetown University Law Center Virtual Conference," USTR Press Office, November 3, 2021.

[5] *See* Global Trade Watch, "Analysis of the NAFTA 2.0 Text Relative to the Essential Changes We Have Demanded to Stop NAFTA's Ongoing Damage," Public Citizen website, accessed December 13, 2022.

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.

"Digital trade" terms that ban data localization requirements would significantly undermine the ability of governments to secure their citizens' data against unauthorized or unlawful exposure or processing, or against cyber-crime, accidental loss, destruction or damage, as these rules would mean consumers have no guarantee that their data would be protected where the data were transferred—even if domestic laws require such protections. Further, countries that have superior privacy laws could see their data protection rules undermined, and U.S. congressional efforts to enact privacy rules could be thwarted.

Concepts prohibiting limits on data flows appear in trade negotiations everywhere from the Trans-Pacific Partnership (TPP) to the Digital Economic Partnership Agreement, to the WTO "e-commerce" talks, and governments are signing up to these terms without understanding the implications for their domestic policymaking. We urge adoption of the precautionary principle when it comes to rules governing the storage of data, and as such, we urge lawmakers to not cement a ban on data localization requirements into binding law.

Limiting Algorithm and Source Code Transparency Requirements

Everyday decisions made by artificial intelligence (AI) components of online platforms affect which individuals and communities can access public and private services. AI uses emotion recognition, facial analysis, and social scoring, often with the intent to materially distort a person's behavior beyond their consciousness and exploit vulnerabilities. Critical components of economic and social stability like home loans, job postings, medical treatments, targeted ads, and much, much more are influenced and determined by AI algorithms, enabling modernized redlining. Governments are likewise increasingly turning to these algorithms developed by private corporations for aid with "predictive policing" and other surveillance functions.[6]

It is clear that there is a huge need for a collaborative effort to address this growing crisis, as demonstrated by the concept of the AI Roadmap, a broad document produced by the U.S.-EU Trade and Technology Council meant to operationalize trustworthy AI.[7] However, in negotiating the terms of such collaboration, the work carried out in the name of "digital trade" should not lead to the lowest common denominator of legal protections for consumers, and as it stands, the AI Roadmap leaves room for unintended consequences with regard to domestic regulation.[8] Instead, all AI systems should comply with mandatory rules that include, but are not limited to, transparency, accountability, and fairness, as well as audits and impact assessments that focus on discriminatory impact, statement of appropriate purpose, and capability.

But "digital trade" terms that require governments to provide trade secret protections for source code and algorithms would limit governments from accessing such information only to instances of known violations of law. Congressional committees, scholars, and public investigators would be barred from reviewing code and related data to identify racist, sexist and other practices deserving of scrutiny and correction. 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.

Undermining Workers' Rights

Corporate surveillance of workers has reached new heights. Workers' activity is being surveilled in and out of work, and their data is being created, collated and sold by and to employers to make managerial decisions. Managers are increasingly relying on source code-protected algorithmic decision systems, allowing employers to sidestep accountability and limit the ability of workers and unions to resist unfair labor practices, discriminatory hiring and firing, and further intrusive surveillance

---

[6] Jane Chung, "Racism In, Racism Out: A Primer on Algorithmic Racism," Public Citizen report, accessed December 13, 2022.

[7] Read the text of the AI Roadmap: *https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management.*

[8] University of Maryland. (December 5, 2022). U.S. Department of Commerce Roundtable for U.S. and European Stakeholders [Video]. YouTube, *https://www.youtube.com/watch?v=MHH6TmAwlEo.*

and monitoring.[9] Data stored by employers is personal and sensitive, including real-time and past physical locations, health information, and more, so we must not make it harder for countries to protect that data via bans on data localization.

Further, there is a false notion that workers providing services online or in the gig economy are somehow different from those in their brick-and-mortar counterparts, and so domestic policies that generally apply to protect the rights of workers do not apply to them. Trade terms such as "discrimination" and "market access" may serve legitimate business concerns, but they can be manipulated by Big Tech companies to disguise attempts to avoid worker protection regulations altogether.

For instance, regulations that require large ride-sharing companies to meet driver hours-of-service rules or to contribute to drivers' social security have been illegal "trade barriers." Big Tech corporations allege such industry standard regulations to be applying "burdensome measures" that impose "unilateral regulations or taxes that deviate from global norms and single out digital platforms for special treatment, often with the intention of giving domestic companies an advantage."[10] Similarly, government action that shuts down operations of a company in their territory due to violations of local labor laws have been characterized by Big Tech companies as illegal limitations to "market access."

Additionally, firms like Google and others [11] are seeking trade terms that would bar governments from requiring a local representative or office as a condition for doing business, which could make enforcement of local labor laws that much more difficult.[12] In the case of unsafe labor practices, if a foreign-owned company is not required to have a local representative, the authorities' only option would be to enforce labor laws against the gig worker themselves, not their employer. Local legal entities therefore are extremely useful for holding corporations accountable to their workers, consumers, and more.

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.

Shielding Online Platforms from Corporate Accountability

Some pacts with "digital trade" rules require governments to enact liability shields for online firms that allow them to evade responsibility for discriminatory conduct, online racial incitement, and other civil rights violations.

The rules that govern the Internet are still hotly debated, particularly Section 230 of the 1996 Communications Decency Act.[13] Section 230 states that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. Online platforms use this law to claim they are not liable for content posted by third parties; for example, fraudulent or defamatory posts on Facebook. Some experts argue this is a core component of free speech online, while others say it mainly serves Big Tech companies to avoid liability for negligence.

There is vigorous opposition to and support for Section 230 by Democrats and Republicans. Such contentious, still-debated issues should not be locked in via a trade agreement, but should be decided in an open and democratic forum. Policymakers must have flexibility to address concerns with Section 230, not have the expanding digital policy space preempted by international trade agreements. Using trade pacts to prevent signatory countries from determining the best ways to protect the public interest online is unacceptable.

---

[9] Duncan McCann, "e-Commerce: Free Trade Agreements, Digital Chapters and the Impact on Labour," International Trade Union Confederation, published April 30, 2022, accessed December 13, 2022.

[10] Internet Association, "Comments Regarding International Internet Priorities," Comment Submission to the National Telecommunications and Information Administration, published July 20, 2018, accessed December 13, 2022.

[11] Google, "Comments Regarding the Indo-Pacific Economic Framework, Comment on FR Doc # 2022–05206," International Trade Administration, published April 11, 2022, accessed December 13, 2022.

[12] Duncan McCann, "e-Commerce: Free Trade Agreements, Digital Chapters and the Impact on Labour," International Trade Union Confederation, published April 30, 2022, accessed December 13, 2022.

[13] Anna Edgerton, "Tech Liability Shield Has No Place in Trade Deals, Groups Say," Bloomberg Law, published May 27, 2021, accessed December 13, 2022.

Undermining Antitrust Regulation

In October 2020, the House Judiciary Committee's Subcommittee on Antitrust, Commercial, and Administrative Law published a report on the monopolistic practices of the four largest tech firms: Apple, Amazon, Alphabet, and Facebook (now Meta).[14] The report concluded that the dominant platforms have:

- Consolidated segments of the digital marketplace and abused monopoly power by advantaging their own products and services on their platforms over independent or smaller ones;
- Acquired hundreds of companies within the past decade, including purchasing potential competitors and shutting down or discontinuing services to foreclose the market; and
- Developed and acted on a financial incentive to abuse their significant and durable market power.[15]

Big Tech companies seek "digital trade" terms that ban limits on size, services offered, or break-ups. As corporations and conglomerates exert increasing control over important social functions, governments must have the authority to combat anticompetitive business practices, place limits on corporate mergers, and break up monopolies where warranted.

In further manipulation of trade rules to undermine worker and consumer safety, there is a concerning trend of encouraging U.S. trade officials to consider other countries' enforcement of their domestic laws to be "discriminatory" if such laws affect U.S. Big Tech companies more than the tech companies from other countries. But sometimes laws of general application addressing market concentration might impact U.S. firms because they have monopolized the industry. For example, Apple and Google are pushing U.S. trade officials to challenge a Korean antitrust law to end anti-competitive App Store practices, claiming the law is "discriminatory" because, due to their monopoly practices, it would affect them more than other businesses.[16]

The United States federal government has a long history of intervening when mergers and consolidations have reduced competition to protect workers' safety, consumers' rights, and economic health. Manipulating trade rules for the consolidation of corporate power does not fit into the Biden administration's new approach to trade policy that empowers workers, defends their rights, and stops the global race-to-the-bottom. 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, nor otherwise restrict the regulation or break-up of Big Tech monopolies.

In addition to the efforts to include binding standards in future trade agreements, U.S.-based Big Tech companies are seeking assistance from the U.S. government in their quest to undermine robust consumer and social protections in other nations.[17] These efforts can be seen in the annual USTR National Trade Estimates report that identifies other countries' laws that Big Tech firms (among others) don't like.[18] In the Biden administration, Big Tech has made the greatest inroads with the U.S. Commerce Department, which has intervened repeatedly—and with deleterious impact—in the EU's adoption of a new digital services regime.[19] Congress should oppose inappropriate U.S. efforts to undermine these kinds of regulatory frameworks, which the United States should in fact be emulating.

Need for Pro-Consumer Rules

There are some legitimate international trade concerns associated with e-commerce and the broader digital economy that should be considered in IPEF or other trade

---

[14] Rep. Jerrold Nadler, Rep. David Cicilline, "Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations," Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives, October 2020, accessed December 13, 2022.

[15] *Ibid.*

[16] David McCabe, Jin Yu Young, "Apple and Google's Fight in Seoul Tests Biden in Washington," *New York Times,* published August 23, 2021, accessed December 13, 2022.

[17] *See* Letter from the Transatlantic Consumer Dialogue to Speaker Pelosi and Leader Schumer, dated June 9, 2022.

[18] *See* United States Trade Representative, "2022 National Trade Estimate Report on Foreign Trade Barriers," published March 31, 2022, accessed December 13, 2022.

[19] Samuel Stolton, "Raimondo: U.S. has 'serious concerns' about EU digital rules," PoliticoPro, published December 8, 2021, accessed December 13, 2022.

negotiations. If digital trade rules are to be included, they should instead ensure that goods purchased online across borders meet labor, environmental and consumer safety standards, including by raising *de minimis* levels so that, for instance, the two million packages arriving from China to the U.S. daily to fulfill online orders can no longer evade U.S. inspection regimes.[20] They should prevent corporate misclassification so that so-called "digital platforms" involved in transportation, hospitality, healthcare, retail, education and other industries cannot evade labor, consumer and other regulations imposed on "brick-and-mortar" businesses. 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.

Transparency and Oversight

Congress and the public must monitor, investigate, and publicly debate the "digital trade" terms that may be sought by Big Tech firms in the context of the IPEF, U.S.-Kenya STIP or other trade negotiations, to ensure that 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 a trade pact 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.

Instead, Congress should insist that the U.S. Trade Representative and the Department of Commerce replace the past secretive trade negotiation process with an on-the-record public process, including public hearings, to formulate U.S. positions and obtain comment on draft and final U.S. text proposals. U.S.-proposed texts and draft consolidated texts after each negotiating session 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 President Biden's 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 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.

[20] Rep. Earl Blumenaur (D–OR), "Chairman Blumenauer Unveils New Legislation to Fix Import Loophole, Level Playing Field, and Boost Oversight," Congressional Press Release, January 18, 2022.