S. HRG. 115–375

THE NEED FOR U.S. LEADERSHIP ON DIGITAL TRADE

HEARING

BEFORE THE

JOINT ECONOMIC COMMITTEE
CONGRESS OF THE UNITED STATES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 27, 2018

Printed for the use of the Joint Economic Committee

U.S. GOVERNMENT PUBLISHING OFFICE
31–138 WASHINGTON : 2018

JOINT ECONOMIC COMMITTEE

[Created pursuant to Sec. 5(a) of Public Law 304, 79th Congress]

HOUSE OF REPRESENTATIVES
ERIK PAULSEN, Minnesota, *Chairman*
DAVID SCHWEIKERT, Arizona
BARBARA COMSTOCK, Virginia
DARIN LAHOOD, Illinois
FRANCIS ROONEY, Florida
KAREN HANDEL, Georgia
CAROLYN B. MALONEY, New York
JOHN DELANEY, Maryland
ALMA S. ADAMS, PH.D., North Carolina
DONALD S. BEYER, JR., Virginia

SENATE
MIKE LEE, Utah, *Vice Chairman*
TOM COTTON, Arkansas
BEN SASSE, Nebraska
ROB PORTMAN, Ohio
TED CRUZ, Texas
BILL CASSIDY, M.D., Louisiana
MARTIN HEINRICH, New Mexico, Ranking
AMY KLOBUCHAR, Minnesota
GARY C. PETERS, Michigan
MARGARET WOOD HASSAN, New Hampshire

COLIN BRAINARD, *Executive Director*
KIMBERLY S. CORBIN, *Democratic Staff Director*

CONTENTS

THE NEED FOR U.S. LEADERSHIP ON DIGITAL TRADE

WEDNESDAY, JUNE 27, 2018

UNITED STATES CONGRESS,
JOINT ECONOMIC COMMITTEE,
Washington, DC.

The Committee met, pursuant to call, at 10:00 a.m., in Room 1100, Longworth House Office Building, the Honorable Erik Paulsen, Chairman, presiding.

Representatives present: Paulsen, Beyer, Schweikert, Adams, Handel, and LaHood.

Senator present: Klobuchar.

Staff present: Colin Brainard, Ted Boll, W. Gavin Ekins, Ryan Elul, Alaina Flannigan, Natalie George, Colleen Healy, Matt Kaido, and Allie Neill.

OPENING STATEMENT OF HON. ERIK PAULSEN, CHAIRMAN, A U.S. REPRESENTATIVE FROM MINNESOTA

Chairman Paulsen. I call this hearing to order.

Every day, when Americans sit down to order goods from a website or consume media online, we are participating in a vibrant digital economy, an economy that takes the ideas and creations of artists, manufacturers, and innovators and puts them within reach of our couches and our kitchens.

Digital trade means supply-chain tracking, 3D printing, or digital platforms that lead to e-commerce, cloud computing, and social media.

You know the names of the leaders in each of these areas; Facebook, Amazon, eBay, and so on. That is because the United States has pioneered this digital revolution. What many don't realize is that trade in manufacturing goods is itself a part of the digital economy. From the websites that market the goods to the payments processing systems that carry out the transaction, the digital economy facilitates the movement of all kinds of consumer products from warehouses to family homes. American manufacturing relies on e-commerce and digital trade.

The benefits of digital trade include domestic economic growth, as well as spreading American ideas and culture across the world. Of course, to us, this is good. Yet there are others who consider the free flow of information, products, and ideas a threat to their control. And nearly three decades after the Berlin wall fell, the way ideas and goods travel from one nation to another remains a contentious issue both politically and legally.

In fact, because of the novelty of digitalization, commercial principles and freedoms that were carefully developed for conventional trade and gained international consensus are now at risk of being circumvented. With every innovation comes opportunity for economic advancement but also opportunity for some foreign governments to grow their own power. In today's interconnected economy, they can have wide ranging effects on international commerce and other national economies as well as the free flows of information.

Digital technology does raise legitimate privacy and cybersecurity concerns, but some governments may not be sufficiently concerned with the effects of their policies on trade, and some may even be using these concerns as an excuse to be protectionist and for other purposes.

Some foreign governments impose additional taxes and fees, and some governments will only permit sales on the condition of storing data locally or providing the source code that will inevitably be used for a competing state-backed product. Some governments that otherwise enforce property and contract laws turn a blind eye to or even facilitate intellectual property theft. This is especially true when the division between the state apparatus and the private sector is nonexistent.

Up on the screen right now, on the right, is a map of the world showing the prevalence of digital trade barriers. The lighter color regions, like Australia, Canada, and Mexico, are perceived to have taken a light-handed approach to trade barriers. And at the other end of the spectrum are trading blocs in countries like the EU and China that make access to their markets far more difficult and costly. In part, their motivation likely is to catch up to the United States, the leader in digital technology development, and try to take the lead themselves.

American companies have always thrived in a competitive market, but the competition must be fair and free from foreign government intervention on behalf of their domestic companies. That is why global players with large economies, such as Chinese and the European Union, which represents large global market shares, should see the rewards of developing their own digital economies without discriminatory standards and testing requirements, localization requirements, forced technology transfers, and the like.

Governments with control over market access should not use their leverage to extract concessions from companies in competition with one another.

In the decades after World War II, U.S. companies dealt with smaller economies that saw the likely economic benefit of opening their marketplace, and their citizens benefited from more choice, lower prices, and faster economic growth, and we must be vigilant to preserve the principles that have already led to greater prosperity throughout the world in the digital trade arena.

And that means addressing swiftly and clearly the excessive burdens foreign governments place on American digital products so that we are not unfairly disadvantaged and can compete on merits.

That also means negotiating new agreements that protect not just America's economic interest but allow the free exchange of culture and ideas throughout the world. The world is a better place,

thanks to American ideas in commerce. Keeping the global digital marketplace open means continuing the fight for that better world.

And before I introduce our witnesses today, I will now yield to Representative Beyer for his opening remarks.

[The prepared statement of Chairman Paulsen appears in the Submissions for the Record on page 28.]

OPENING STATEMENT OF HON. DONALD S. BEYER, Jr., A U.S. REPRESENTATIVE FROM VIRGINIA

Representative Beyer. Thank you, Mr. Chairman, very much.

Since this committee took up digital trade last fall, President Trump has weighed into the trade issue in unpredictable and destabilizing ways. The President's erratic, aggressive approach has created an environment of economic uncertainty, is alienating our trading partners and allies, and risks harming the global economy.

So far, the President's trade advisers have seemed uninterested in the significant majority of the U.S. economy that does not consist of heavy manufacturing. Not only has digital trade not been front and center, it seems the Administration simply does not have a strategy for how to strengthen U.S. leadership in digital trade nor any interest in creating one.

Ceding ground to others, including the competitors who are putting up new barriers, hurts our economy and our workers. This failure to lead is a missed opportunity for U.S. small businesses, technology companies, manufacturers, and farmers, and all who benefit from the increased export opportunities made possible by digital trade. It also risks the United States falling behind as other countries race to create the technology of the future and write rules for operating in the digital economy.

Strengthening our position in digital trade starts right here at home by ensuring an open internet that enables innovation to flourish.

To that end, it is critical that we restore network neutrality, which is vital for small business owners who rely on the internet to compete with bigger companies. It also means expanding access. Too many people still don't have access to a broadband connection, and their ability to compete in an increasingly digital economy is undermined without high-speed internet.

We need to keep our focus on creating opportunities for all Americans. As we are here this morning, the digital playing field around the globe is far from level. When dealing with China, American companies confront rampant theft of U.S. intellectual property, force technology transfer policies, data localization requirements, and other efforts to tilt the playing field against the United States.

Equally concerning, China is becoming a model for other countries who are erecting trade barriers that restrict the free flow of data. We need to knock down these barriers in a systematic, thoughtful way, rather than pursuing a policy of ill-conceived tariffs that create additional barriers to trade.

Further, some data regulations are particularly onerous for small and medium-size firms that don't have big IT departments or can't absorb the added cost of having to store the data locally or comply with other requirements.

Digital trade is just one piece of a broader trade landscape. In the last few months, it has been harder and harder to understand the Administration's position on a range of trade issues.

One Wall Street analyst estimates that the Administration's erratic trade policies have cut the value of U.S. equities by $1.25 trillion. And the costs extend far beyond the stock market. The Administration's tariff on solar panels will cause the loss of thousands of jobs and the delay or cancellations of billions of dollars in investment in solar energy. These tariffs will slow our transition to renewable energy.

The Administration has used dubious national security justifications to levy counterproductive tariffs on our closest allies. The President has repeatedly acknowledged that these tariffs are not justified by national security concerns, undermining any future U.S. case of the WTO.

By levying these tariffs, he has managed to damage our economy and our alliances in one fell swoop. And, of course, the negative aspects of President Trump's trade policy are compounded by his dyspeptic approach to diplomacy. And nowhere was this clearer than his catastrophic performance at the G7 in Charlevoix.

Public expressions of disdain for our leaders of our democratic allies will only make them less likely to engage in productive trade negotiations. As the President becomes increasingly unpopular abroad, it becomes difficult for democratic leaders to engage in new agreements with the United States.

We need a trade policy that is guided by principle, not whim; that is forward looking, not reactionary; something that we saw from previous administrations.

But that is not why we are here today. The way President Trump has gone about renegotiating NAFTA has generated instabilities, fighting almost daily with Canada, as threats to leave the NAFTA deal risk disrupting markets, raising prices, and may trigger retaliatory tariffs.

Rather than pursue productive discussions with China to drive changes in their trade practices, President Trump has launched a trade war rolling up $50 billion in tariffs and threatening another $200 billion in tariffs last week.

China, of course, immediately promised retaliatory tariffs of the same scale. Even the President's Council of Economic Advisers prepared an internal analysis showing that tariffs will harm our economy. You know, trade is often a ripe barrier for bipartisan agreement, and that is often especially true in the area of digital trade. But the damage to trading relationships with the Administration's moves to impose tariffs on steel, aluminum, and other products harms the United States' ability to forge partnerships that will expand trade both online and offline. And that uncertainty has a chilling effect on trade of all kinds.

We have only begun to see the damage from Trump's trade policies.

I really look forward to hearing from the witnesses today how we could promote digital trade, how we can knock down barriers, and how the Administration can play a more constructive role in expanding American trade.

Mr. Chairman, I yield back.

[The prepared statement of Representative Beyer appears in the Submissions for the Record on page 29.]

Chairman Paulsen. Thank you.

And now with our four witnesses here today, we will start with Mr. Sean Heather, who is the vice president of the U.S. Chambers Center for Global Regulatory Cooperation. He also serves as Executive Director for both international policy and antitrust policy.

During his 15-year career at the chamber, he has worked on a number of diverse issues such as international trade and investment, taxes, standards, technology, and corporate governance. Before joining the chamber, he worked for the Illinois comptroller and with several political campaigns across the State.

He holds an undergraduate degree and a Master's of Business Administration from the University of Illinois.

Mr. Ryan Radia is a Research Fellow and Regulatory Counsel at Competitive Enterprise Institute. His research encompasses intellectual property, information privacy, and cybersecurity.

Mr. Radia has published extensively in major news outlets, appeared on dozens of national shows, and contributes to several blogs on policy and technology.

Mr. Radia holds a Juris Doctor from the George Washington University Law School and a Bachelor of Arts in Economics from Northwestern University.

Ms. Rachel Fefer is an Analyst in International Trade and Finance at the Foreign Affairs Defense and Trade Division of the Congressional Research Service where she focuses on digital trade and the World Trade Organization.

Before joining the Congressional Research Service, Ms. Fefer worked at the Department of Commerce and the Food and Drug Administration on trade issues. Previously, she worked in the private sector for various tech companies in the private sector. Ms. Fefer holds a Master of Business and a Bachelor of Arts in Public Policy from Duke University.

And also joining us is Ambassador Robert Holleyman, who is the President and CEO of Crowell & Moring International, as well as the Partner in Crowell & Moring's International Trade Group.

He served as Deputy U.S. Trade Representative between 2014 and 2017. And during this time, Ambassador Holleyman was responsible for trade policy and services, investment, and intellectual property, and led the creation of the digital trade working group within the Office of the U.S. Trade Representative.

He received his Juris Doctor from the Louisiana State University Law School and a Bachelor of Arts from Trinity University in San Antonio, Texas.

And, with that, we will welcome and begin our testimony with you, Mr. Heather. You are recognized for your statement of 5 minutes.

STATEMENT OF SEAN HEATHER, VICE PRESIDENT, CENTER FOR GLOBAL REGULATORY COOPERATION, U.S. CHAMBER OF COMMERCE, WASHINGTON, DC

Mr. Heather. Thank you, Mr. Chairman and Ranking Member and members of the committee, for inviting me to testify.

In previous testimony to this committee, I highlighted how certain governments are unnecessarily restricting digital commerce and seeking to undermine American technological innovation. Restrictions on cross-border data flows via forced localization measures, new complex and burdensome regulatory regimes, problemsome customs approaches to e-commerce, and investment measures that force tech transfer are some of the most common digital challenges that American companies face in foreign markets.

Advancing American interest in the global digital economy needs to be a top international priority, and we need a whole-of-government approach to counteract trade and regulatory barriers to digital goods and services.

This starts by recognizing the importance of services. Without question, American manufacturing is a big part of the digital economy, whether simply sold through e-commerce channels or part of the growing number of products that make up the Internet of Things. However, we must not overlook our dominant position in services. And the internet is making services more tradeable every day.

The United States is the world's largest exporter of services, and we enjoy a trade surplus in services of nearly $250 billion. Moreover, services sales by foreign affiliates of U.S. multinational corporations tops $1.4 trillion.

Despite these big numbers, the potential for services industries to engage in international trade is almost untapped.

One in four U.S. factories export. But just 1 in every 20 providers of business services export. This means only 3 percent of U.S. services output is being exported. Therefore, our support for digital trade starts with increased support for our service industries.

Now, let me turn to the importance of the State Department and the Department of Commerce.

Foreign embassies are the first line of defense against impediments to digital trade and are important messengers for a liberalized approach to digital economy. The Bureau of Economic and Business Affairs at State plays a central role in coordinating U.S. engagement on ICT and cyber policy matters.

Likewise, the Department of Commerce plays a critical role in advancing U.S. digital exports and advocating for the adoption of U.S.-friendly digital regulatory frameworks. It also has a core responsibility to safeguard the voluntary private sector approach to standards that underpins many ICT products.

Since its inception in 2016, working with the State Department, the Commerce Department has operated a valuable Digital Attache Program that embeds U.S. digital policy experts in key U.S. Embassies. Expanding this program, ensuring adequate resources, and giving them a clear mandate to focus on digital trade is critical to ensuring American leadership in the digital economy.

Further, State and Commerce should lead a whole-of-government effort to support international privacy and cybersecurity frameworks that facilitate the seamless movement of data across borders. We applaud the Administration for efforts last year to ensure the EU–US Privacy Shield successfully made it through its first annual

review. And we look forward to supporting this review this year post Europe's implementation of GDPR.

However, Privacy Shield is just one approach. The United States has importantly also advanced, within APEC, the Cross Border Privacy Rules to promote the movement of data between borders and bridge national privacy regimes. The United States should do more to encourage APEC governments to join. Further, it is important to develop similar mechanisms within other regions of the world, including Latin America.

While differences between privacy regimes can be bridged increasingly, cybersecurity regulatory frameworks are being developed that also threaten the movement of data.

The United States has created the NIST Framework, an innovation-friendly framework to manage cyber risks. However, approaches developed in foreign jurisdictions often look much different. The United States needs to be more active in both shaping and aligning these emerging regulations but also developing new agreements to address cross-border cybersecurity requirements.

Turning to trade agreements, the Chamber sees the need to seek commitments from our trading partners to support digital trade in goods and services and foster cross-border movement of data.

We welcome USTR's efforts to modernize NAFTA to include digital trade provisions. We also strongly support the United States playing a leading role within the WTO to develop e-commerce rules that ensure an open and predictable marketplace for American businesses.

We would also encourage the Administration to consider relaunching negotiations around the Trade in Services Agreement, otherwise known as TiSA. TiSA has the potential to be more than just a services agreement as it could secure data flow commitments to the benefit of all sectors.

Finally, while USTR, Commerce, and State play focal roles in developing and advocating the U.S. digital strategy, U.S. regulators are very much needed for a whole-of-government approach to be effective.

The Federal Trade Commission has been active with the Department of Commerce to advance an understanding of U.S. privacy protections in shaping foreign privacy laws and in being the enforcement behind data flow agreements like Privacy Shield. But other U.S. regulators are increasingly being called upon. U.S. financial regulators need to be there to ensure regulatory frameworks abroad don't limit U.S. opportunities for fintech leadership.

U.S. auto and aviation regulators also need to be there to encourage that regulatory designs abroad will not affect American competitiveness on things like autonomous vehicles and drones.

Further, regulators in foreign markets are beginning to contemplate policy questions about artificial intelligence, machine-based decisionmaking, access to algorithms, and big data, as well as a host of other issues. U.S. regulators need to be at the ready to positively shape these discussions.

In whole—or in short, a whole-of-government approach requires the entire U.S. Government to be vigilant, coordinated, better prepared to actively shape foreign regulatory environments that will deeply impact Americans' ability to compete abroad.

With that, I thank you for the opportunity to testify and look forward to your questions.

[The prepared statement of Mr. Heather appears in the Submissions for the Record on page 31.]

Chairman Paulsen. Thank you.

And, Mr. Radia, you are now recognized for 5 minutes.

STATEMENT OF RYAN RADIA, RESEARCH FELLOW AND REGULATORY COUNSEL, COMPETITIVE ENTERPRISE INSTITUTE, WASHINGTON, DC

Mr. Radia. Thank you, Chairman Paulsen, Representative Beyer, members of the Committee. We are at a critical juncture for international trade. And at this time, the United States must maintain its historic role as a global leader and promote free trade in open markets.

I will focus specifically on the information economy. The U.S. technology sector is not just important domestically, but it exports $300 billion annually in products and services, supporting 800,000 American jobs.

Tariffs and nontariff barriers to trade do risk trade in the digital marketplace. I will focus on another set of policies, however, that threaten digital trade; governmental regulations regarding privacy copyright and antitrust.

Particularly important is the European Union. Their member states collectively represent America's single largest trading partner in goods and services. And there are 430 million Europeans who use the internet, meaning that Facebook has more European users than American users. Google is more popular as a search engine in Europe than it is the United States. The same is true for tech companies of all sizes. So, although EU users are a core aspect of the user bases of United States technology companies, the EU, European Union's approach to regulation differs dramatically from that in the United States, underscoring the need for greater U.S. leadership in this space.

In particular, the European Union, as Mr. Heather mentioned, recently implemented the GDPR, the General Data Protection Regulation. It went into force on May 25, 2018, and in just over a month, it has already had major effects on how digital trade occurs between the United States and the European Union. Those effects, I believe, will only grow.

The GDPR applies to any company that processes or controls data on EU data subjects, no matter where the company is domiciled and, in some cases, regardless of the size of that company. The GDPR does not distinguish between offline and online data collection, but the brunt of its impact will be felt, and is being felt, by technology companies and financial companies.

So far, some of the most notable examples of the GDPR include U.S. companies stopping providing service to EU users for fear of regulatory fines, which in the EU could amount to up to 4 percent of a firm's global revenue. Tronc, formally Tribune Online, has stopped serving EU users with websites like the Chicago Tribune, the Los Angeles Times. A&E Networks followed suit. An internet analytics firm called Klout that helps social media users and thinkfluencers gauge their reach shut down its operations entirely

on May 25th, the day the GDPR went into force. Many other examples, not just in the United States but around the world, have occurred.

The result of this is not just harmful to the EU users who will lose out on American content and American companies who will lose out on revenue from EU users. Even those who comply with the regulation will have a more difficult time monetizing their content. But also it hurts U.S. consumers because in this industry, where fixed costs are high and the marginal cost of delivering content to consumers is low, any reduction in revenue from a major user base means a reduction in the quality of overall service.

So the cost of compliance with the GDPR will likely be significant. According to estimates from Ernst & Young and the International Association of Privacy Professionals, the average Fortune 500 spent $16 million to comply with the GDPR in the 2 years before it went into effect. It seems that the cost of complying with this regulation will only increase.

Moreover, the GDPR may entrench existing internet companies at the expense of startups because large established companies that could not have complied with the GDPR when they were in a dorm room or a garage are now better positioned to do so.

The role of U.S. leadership in this space is important. Congress has been considering a number of bills to address privacy. Although I won't discuss the specifics of those bills, it is important that Congress and the Administration take a lead in advocating an approach to user privacy and data protection that recognizes the need to reduce compliance costs, that respects the role of notice and choice, and does not put onerous mandates on businesses.

In brief, a couple of other areas in which EU policies are harming or potentially risking harming U.S. business include the European digital single market's treatment of copyrighted materials. In general, the European Union's digital single market is a laudable effort to harmonize regulations and taxes across EU member states, but it has also created and will continue to create barriers and restrictions on practices, such as geo-blocking and different treatment of content by content owners in the movie industry, streaming platforms, and the like, ultimately hurting consumers.

Similarly, the European Union's approach to competition policy has targeted U.S. companies. Record-breaking fines against companies such as Intel, Google, and Microsoft, several of which are still under appeal in the EU courts, have undermined American companies and represent a seeming effort by the EU to engage in protectionism.

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

[The prepared statement of Mr. Radia appears in the Submissions for the Record on page 38.]

Chairman Paulsen. Thank you, Mr. Radia.

And Ms. Fefer, you are recognized for 5 minutes.

STATEMENT OF RACHEL FEFER, ANALYST, INTERNATIONAL TRADE AND FINANCE SECTION, CONGRESSIONAL RESEARCH SERVICE, WASHINGTON, DC

Ms. Fefer. Chairman Paulsen, members of the Committee, thank you for the opportunity to testify today. My testimony focuses on the increase in digital trade barriers around the globe and how other countries are shaping new international standards and rules that may impact the market access for U.S. firms.

The internet-driven digital revolution is causing fundamental changes to the U.S. and global economy. According to the U.S. International Trade Commission, in 2016, the digital economy supported 5.9 million U.S. jobs. The United States is a leader in international digital trade.

U.S. firms Google, Microsoft, Amazon, and IBM are top global cloud service providers. At the same time, challenges exist that may impede the growth of digital trade.

Multiple U.S. public and private sector reports identify a breadth of digital trade barriers, including high tariffs, localization requirements, such as cross-border data flow limitations, intellectual property rights infringement and forced technology transfer.

Congress has taken an interest in addressing trade barriers. In 2015, Congress set negotiating objectives for trade agreements to include provisions such as World Trade Organization's nondiscrimination provisions to digital trade, and to prohibit forced localization requirements and data flow restrictions.

The proposed Trans-Pacific Partnership included these provisions and others, and multiple opportunities exist to pursue these objectives in ongoing negotiations as highlighted in my written submission.

No single set of international rules or disciplines governs digital trade. This lack of globally accepted rules and standards means that individual economies around the world are creating their own, experimenting with different approaches.

I will focus on how China and the European Union, or EU, are each shaping global norms. China has a fundamentally distinct approach to the internet. With over 700 million internet users and the world's largest market for e-commerce, China is attractive for many U.S. businesses. However, China's various government policies and actions have limited the ability of U.S. firms to compete there. For example, China's policy of internet sovereignty censors or limits what websites or data individuals can access. China's cybersecurity law restricts cross-border data flows and requires safety reviews of critical network equipment. Many U.S. firms are concerned that this law may lock them out of the market or force them to transfer proprietary technology or information to Chinese regulators or partners.

The EU poses a different type of challenge for U.S. firms. Its legal approach to information privacy and protection of personal data has led to policies that vary from those of the United States. As mentioned, the EU's General Data Protection Regulation, or GDPR, took effect last month. It establishes a single set of rules for personal data protection throughout the EU and grants individuals new rights to control their data.

U.S. firms have voiced several concerns about the GDPR, including its complexity, how it is implemented and enforced, and the scale of potential fines. Some U.S. firms exited the EU market rather than comply with the regulation. Because no multilateral rule exists on cross-border data flows or data privacies, some experts state that the GDPR may effectively set new global data privacy standards.

Countries such as Brazil, Japan, and South Korea consulted with the EU for their own data protection laws. Some U.S. firms determined it is easier to comply with EU regulations globally rather than implement changes only for the EU market. U.S. privacy advocates and others support these decisions.

Some analysts view China and the EU as using their large market size to impose their views and set global rules. They contend that the United States should proactively counter their efforts. Others suggest that the United States should focus on developing new digital trade rules and disciplines through trade negotiations.

Mr. Chairman, thank you again for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Ms. Fefer appears in the Submissions for the Record on page 47.]

Chairman Paulsen. Thank you.

And now we will hear from Ambassador Holleyman. You are recognized for 5 minutes.

STATEMENT OF AMBASSADOR ROBERT HOLLEYMAN, FORMER DEPUTY U.S. TRADE REPRESENTATIVE, OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE (USTR), WASHINGTON, DC

Ambassador Holleyman. Thank you, Chairman Paulsen, Mr. Beyer, members of the Committee. I appreciate the opportunity to testify before you today. I have three points I would like to make.

First is that U.S. leadership in digital trade isn't about technology. And it is not just about the technology industry. Digital trade is the tool by which every business competes. Whether you are a home enterprise or managing a supply chain or you are accessing a market, it is fundamental. And I share the view of your Vice Chairman, Senator Lee, from your earlier hearing where he said that we are swiftly approaching a point where the word "digital" will be an unnecessary adjective for trade. Digital underpins every aspect of our economy. And I think it is critical for us to recognize that part of the digital transformation because it also talks about why this issue in your hearing is imperative for U.S. industry and long-term leadership.

I just returned from Hong Kong and Beijing. And I could tell you the fast pace at which foreign competitors to U.S. technology leaders and U.S. companies who rely on technology are gaining ground quickly. And as one foreign government official said to me, he said, "I am not sure people in the U.S. fully realize how much in Asia that non-U.S. technology providers and platforms are gaining an edge over, in many case, U.S. firms." We are still the leaders but the competitors are catching up very quickly.

We have had discussions about the rules that foreign governments are setting up that impact this, and I will be happy to an-

swer questions. I think our fellow panelists have discussed this well. One of the things that we did at USTR under the leadership of Ambassador Mike Froman, was create a Digital Trade Working Group to try to bring the entire USTR approach on focusing on this—not just the tech people, not just the people from one region, but we wanted essentially a SWAT team so that if we saw a digital trade barrier being erected, we could move quickly to try to address that.

And one of the key factors we did was asked the International Trade Commission to undertake a three-part study that looked at the impact of digital trade barriers. It has already been referenced. The first study came out last August. It was intended to really look at the scope of this. The next two studies are to look at B2B digital trade; the next, B2C, business consumer digital trade. And they are intended to be providing our negotiators and Congress with information about which aspects of this are the most impacted by regulations, which are sectors that are important now but long-term will be part of the underpinning of American competitiveness, and allow USTR and this Congress to help prioritize in fighting digital trade barriers.

My second point is that we have to continue to lead. And this was a practice, you know, we focused on—broad bipartisan support. I would say that not only is the Administration's current approach on trade causing uncertainty within the business community, but it is also, it might be crowding out the attention that should also be focused on digital trade.

We need our allies working with us to break down these barriers. We need to flex our muscle to show in the trade landscape that we have a better approach to digital trade. There are several models I am happy to talk about. The broadest model is now what we are not only trying to do at NAFTA, but what, you know, the 10 trading partners are trying to do in the comprehensive and progressive Trans-Pacific Partnership, which is the model.

Finally, I will talk about a big opportunity, which is privacy. We have heard a lot, and I agree with the statements about how the European Union with their comprehensive approach to privacy through the GDPR, which went into place last month, has really begun to set the global framework around the approach to privacy.

But there is an alternative, and it is actually an alternative that America helped endorse, which is the Asia-Pacific Economic Cooperation forum Cross Border Privacy Rules. That is an approach that is the U.S. and 20 other economies of how you would transfer data around the Asia-Pacific region. The U.S. has supported this. It is important for us, for this committee, and others to do everything possible for the U.S. to encourage our trading partners in APEC to stand up and put in place those Cross Border Privacy Rules that have an Asia-Pacific and an America supported framework for privacy as a counterpoint to what the EU is doing.

With that, I am happy to answer any questions you have, but we should not take a back seat to any country in our leadership on these issues. And I appreciate the important role of this Committee in shining a light on digital trade. Thank you.

[The prepared statement of Ambassador Holleyman appears in the Submissions for the Record on page 62.]

Chairman Paulsen. Thank you, Ambassador Holleyman.

I will ask that members do keep their questions to 5 minutes, and I will begin. I will start with you, Mr. Heather.

The EU's General Data Protection law, or GDPR, which several of you actually referenced, and the notices we have been receiving about it here in the United States are a wake-up call that alerts us to the fact that foreign government actions in their own domestic markets can have a very direct repercussion for us as well.

I have heard from folks in Minnesota, for instance, that have expressed confusion about the complexity, and they are just questioning about where do they go next.

Can you just frame a little bit more about, you know, for the committee here, what are the developments that are taking place in other countries or trading blocs around the world with respect to the governance of digital services and digital technology? Or maybe can you sketch out a little bit about—you talked a little bit about the program with the Department of State and the Department of Commerce, but for us here in the United States, our involvement in this process, how can we be making sure that our interest for our citizens and our businesses is in fact protected?

Mr. Heather. So I think there is a lot there, Mr. Chairman, to respond to.

I think, first of all, what I would say is this: The primary concern around privacy regulations is the ability to move data. The secondary concern around privacy frameworks that we see around the world is the ability to offer the products and services that you have in that market.

So, whenever you are looking at a privacy framework, whether it be in the EU or now in about 120 different jurisdictions around the world that have updated their privacy laws or are in the process of updating their privacy laws, when we evaluate those. We evaluate them on that two-prong test, will this regime limit the ability to move data outside of the country? And, two, how harmful will it be for us to offer the products and services that we would like to offer in that market?

As I think has been discussed here at length, Europe is way ahead of the game in terms of influencing the world around GDPR. Many of the governments around the world have looked to Europe as a model and have taken most of it, not all of it but most of it. Where I think an effort should be made today is on cybersecurity. There is yet to be the race for who defines how cybersecurity laws are written around the world.

Vietnam just put a new law on the books recently that forced localization of data, and oftentimes, these cyber laws are a second bite at really privacy questions.

Here, I think the U.S. has a helpful message in the NIST framework that could be advanced in these foreign markets with discussions with legislators and regulators in those economies. And I think an effort to do more on the cyber front would be imperative because I think that is the next battleground for data flows and questions of forced localization.

Chairman Paulsen. Ambassador Holleyman, let me just follow up because I think Mr. Heather mentioned TiSA as an opportunity in this space. And given your experience at USTR, maybe can you

describe a little bit for the committee how TiSA could be used to advance some of these concepts?

My understanding is that the work that has been done on NAFTA, which obviously has not been completely modernized, has been progressively very well in the area of digital space uses, the model out of TPP that you are involved in, but can you just elaborate maybe for us?

Ambassador Holleyman. Certainly, Mr. Chairman. And the Trade in Services Agreement would be a big opportunity. We were working to negotiate that in our Administration. It is an opportunity to sort of bring new industries together around new frameworks.

Candidly, the challenge around that is also going to be the EU. I mean, their views on data movement and protection are very different from the U.S. I tend to think that we should look at a potential plurilateral agreement around data and around the digital economy and that we should actually align with the TPP partners around the set of data issues. Because their view on data, as they have now adopted, as we are promoting in NAFTA, is essentially the same.

And so I would actually think that would be a faster way for us to set rules on data than the TiSA, which I also think is hugely important for a broader set of industries.

Chairman Paulsen. And, Mr. Radia, would you concur on some of those comments. You mentioned we should not mimic what the EU is doing, for instance, in GDPR.

Mr. Radia. I would concur with those comments that we should stake out a role that emphasizes that customizable agreements between users and companies are important with respect to data localization. Ideally, when companies make decisions about where to store data about particular users, that decision should be made based on efficiency, based on how the technology works, on optimizing the user experience. To the extent that harmonization can occur, that multilateral agreements can occur that ensure that companies don't have an incentive to store data in one place about a user rather than another because they can be subject to a different set of laws, that would help advance innovation and competitiveness.

Chairman Paulsen. Thank you.

Mr. Beyer, you are recognized for 5 minutes.

Representative Beyer. Thank you, Mr. Chairman, very much. And thank you all very much for your testimonies.

Mr. Heather, Tom Donohue, your boss, president of the U.S. Chamber of Commerce, said this spring, quote, the tariffs of $30 billion a year would wipe out over a third of the savings American families received from the doubling of the standard deduction in the tax reform bill.

I know the chamber is very clear in its opposition to tariffs, but last Friday, the Trump Administration detailed $50 billion in tariffs against Chinese imports.

What is going to be the impact on American consumers of this trade war? And aren't higher prices just a different way of essentially raising taxes on them?

Mr. Heather. So I think the Chamber's concerns with the approach to the Trump Administration is taking, both with regard to tariffs, as well as with regard to the approach in renegotiating NAFTA, is well documented in terms of the chamber's objections to the way this Administration is headed. And, yes, we do believe tariffs are taxes on American consumers.

Representative Beyer. Thank you very much.

Ambassador Holleyman, first of all, thank you very much for your service in the USTR.

The Administration is now fighting trade battles with Canada, with Mexico, with Germany, with the WTO, this cozying up to Russia and North Korea. Does the President's seemingly belligerent attitude towards our allies, our trusted trading partners make it more difficult to reach agreement on digital trade issues?

Ambassador Holleyman. Well, we lose our focus through that. I mean, it is hard to prioritize those issues when you are attacking your allies, and that is why I believe we really have to find an approach on digital trade where we find some group. And, quite frankly, that is not only our NAFTA partners, but that is our former TPP partners. And we need to support them as allies in this effort and get focused on those issues rather than, in many cases, treating them as enemies, which is what we are doing, certainly, in the proposed auto taxes and the steel and aluminum taxes.

Representative Beyer. Thank you very much.

Mr. Heather, the administration in China, I know you are very aware, they are going tit for tat on tariffs on everything from agricultural products, steel, electronic components, semiconductors, lithium batteries, given the potential for tariffs on electronic components that are important to building up the digital infrastructure, can you talk about the potential consequences of the existing tariff battle on our ability to move forward on digital trade?

Mr. Heather. I am not a tariff expert. I spend most of my life thinking about nontariff barriers in the regulatory context. But as I said before, tariffs are taxes on consumers, and so the cost for consumers to access digital technologies will inevitably go up.

Representative Beyer. I assume you are distraught, too, about the potential for 25 percent tariffs on all imported cars or banning all German luxury cars.

Mr. Heather. I think our views on 232 are also well documented. We were not supportive of the approach on steel and aluminum. And our concerns associated with where they may be headed with 232 on autos is also on the record.

Representative Beyer. Ambassador Holleyman, restrictions on the cross-border flow of data, the so-called data localization requirements, are immensely costly for U.S. businesses across a wide range of sectors. And countries seem to be imposing these requirements in a supposed effort to protect privacy—you don't have to worry about the NSA—improve cybersecurity, bolster economic growth, but it seems like the data localization effects have exactly the opposite effect.

How can we most effectively, the U.S. Government, U.S. businesses, push back against these?

Ambassador Holleyman. Well, two things: Certainly, the effort, while I don't agree with all the tactics and tools, the effort to

focus on the problems in China is critical. When I was there for a cyberspace trilateral with China, India, and the U.S. think tanks 2 weeks ago, the Chinese very proudly talked about the concept of data sovereignty and why they needed to restrict the information that was coming in and out of the internet, not only for their citizens but for their businesses.

And we have to push back against those. We do have a tool; we have a group of people, group of countries who share that view, led by Japan, Canada, Mexico. We need to align with them because, quite frankly, the Chinese approach is gaining support from other economies who look at that. We need a counterpoint.

Secondly, we have to promote things like the APEC Cross Border Privacy Rules as a viable alternative, which it is, to the GDPR. The U.S. is behind that. Japan is behind it. But we need to get more countries, economies behind it and really drive it because that is part of the answer to ensuring that there is an American-led approach to privacy and cross-border data transfers.

Representative Beyer. Great. Thank you.

Just very quickly. WTO for years has agreed no customs duties on electronic transmission, and now Indonesia seems to be going in a different way. Is there anything specifically we can do to try to change Indonesia from becoming the new role model?

Ambassador Holleyman. Well, one, I think we need to have a sort of plurilateral tool. I think we have to complete NAFTA and show that we have got the cross-border rules there. And, three, I think we have to use our bilateral tools with Indonesia to push back on this and tell them what a break that would be, not only with their neighbors but with the U.S.

Representative Beyer. Thank you very much, Mr. Chairman.

Chairman Paulsen. Thank you.

Representative Schweikert, you are recognized for 5 minutes.

Representative Schweikert. Thank you, Mr. Chairman.

Look, this is fascinating for a lot of us. And one of the interesting things hearing is you are starting to here now both parties being free trade, which is sort of exciting considering our past history in those subjects.

I want to also walk through, because my fear is in this discussion it is much more complex than we are actually touching on. You know, whether it is the Europeans' attempt to—you know, the right to be forgotten, you know, the right to remove data, to how I move a product in a supply chain back and forth, to digital commerce where, what is money? Can I move a cryptocurrency to do a purchase? Can I actually have PayPal, you know, be my mechanisms? Or do I have to touch a SWIFT system that actually has certain bilateral agreements already attached to it, to now to one of my personal fixations is data on supply chains.

And is it Ms. Fefer? Did I get close in the proper pronunciation? You have done some writing about this not too long ago, if I remember correctly.

Am I going the right approach, that part of our issue with Europe is the individual privacy issues, but our issue with certain areas in Asia, it is the control of the money flow and the product supply chain?

Ms. Fefer. Thank you, sir. I think our issues are not so crystal clear, that we have a variety of issues with Europe. I think the most prominent one at the moment I believe is privacy with GDPR. With Asia, a lot of the issues are similar, and revolve around the cross-border data flows, as has been brought up many times, as companies use more and more cross-border data flows for supply chain tracking.

For example, blockchains.

Representative Schweikert. Yeah. Look, as you know, I have a personal fixation on distributive ledger. You know, and within that, we have actually had presentations on you could manufacture a product here, you could actually, you know, use RFID or types of encoded containers, padlocks, to make it much more efficient to move through Customs.

We could, you know, the documentation, so it hits Customs; you already had the manifest that completely loads. But that is operating at one level, but now I have a problem if there is privacy on my ability to have made the order, to move the money, to—was the details in the manufacturing order, was there proprietary information there that doesn't get stolen or handed to the government?

Has anyone out there in all of your experience sort of talked about or written about sort of this unified theory of how we deal with Europeans' privacy concerns, parts of Asia's ability to remove money, our concerns about moving IP? I mean, if we came to you and said, "Where do we go to sort of find this unified theory," who has written on it? And sort of a universal question for everyone on the panel.

Ms. Fefer. As to who has written on it, I would probably need to go back and look a little further, but I believe that a lot of the various organizations that focus on privacy issues or on data flows or that represent the industry have written on this, but I can get back to you on that.

Representative Schweikert. Ambassador Holleyman.

Ambassador Holleyman. I appreciate your focus through the Blockchain Caucus, and I think these issues are critical. I would say I think there are two things: One is the APEC Cross Border Privacy Rules are intended to have a referential that would essentially allow them to be interoperable with EU GDPR. And——

Representative Schweikert. So you believe that one could actually be sort of an international standard, WTO, or however you——

Ambassador Holleyman. It was intended that the two of those should be interoperable and that businesses should be able to work across because, quite frankly, we are not going to get the EU to stand down on their privacy——

Representative Schweikert. That would be more of a privacy standard for—down to the individual level.

Ambassador Holleyman. Well, around personal information.

Representative Schweikert. Yes.

Ambassador Holleyman. Personally identifiable information, which is replete in what large businesses have. So I think that is an important part of that.

Secondly, you know, the role of blockchain technologies, which I think is huge in terms of not only supply chain efficiency but elimi-

nating corruption in government systems, reducing leakage, and right now, the rules, because they are so diffuse, don't fully ensure that a country like China couldn't simply block new technologies and require that a domestic——

Representative Schweikert. And I have only—Ryan? Sorry. I really liked parts of your testimony, and you hit some really brilliant things, but is there any platform because, you know, we were all so excited a few years ago, the ability to use internet and public information to deal with everything from baksheesh—I mean, corruption in societies. And I know certain local governments have pushed back on that at the same time you and I are trying to build sort of the eBay of the world. Where do I go to try to find a way to continue to push open commerce?

Mr. Radia. I think that is being explored by a lot of scholars, including the use of the distributable ledger. I would be happy to follow up on projects that are underway in that regard.

Representative Schweikert. If we get a second round, I would love to talk to you about, is a worldwide sort of node network one of the solutions?

Thank you, Mr. Chairman.

Chairman Paulsen. Thank you.

And, Dr. Adams, you are recognized for 5 minutes.

Representative Adams. Thank you, Mr. Chairman.

And thank you all very much for your testimony.

I agree with the idea that the U.S. must lead on the issue of digital trade as it provides the foundation upon which the world's economy of the 21st century will be built. But I want to emphasize that we focus on not repeating the same mistakes we made in past trade agreements like NAFTA, which really impacted my State, which eroded the wages of middle class workers and small business owners. We need to ensure that the benefits that flow from our future trade agreements are shared equally among all market participants.

Ambassador Holleyman, you mentioned in your testimony the trade barriers that foreign nations are enacting in terms of new regulatory regimes and rules in the digital space.

So my question is, how can Congress break through these barriers in a way that ensures U.S. business and workers are able to play on a level playing field, thus ensuring that benefits flow to all?

Ambassador Holleyman. Thank you, Dr. Adams. I appreciate your question.

There are two things I would suggest. One is by using your power in Congress to make sure that these issues are top of mind and top of attention for the U.S. Government. It is not only by having hearings like this, and having the good work of CRS; I also highly commend these International Trade Commission reports. In fact, there are two that will be coming out that are actually going to be confidential.

Ambassador Lighthizer will determine whether any of that is made available, but I would encourage this committee when that is, the next two are made available, to have a classified hearing and ask the ITC because they were really trying to dig into this to help this committee and the negotiators understand where to focus their efforts.

Secondly, I think we have to more broadly bring the benefits of a global trade to our citizens, and I think that is improving things in our local community. But I also think it is fighting among like-minded economies and countries for provisions like the digital 200 that were in the TPP and that are similar in NAFTA, allying with our partners and moving ahead with those. Because until we get new rules in place, then we don't have an effective counterbalance against the economies that want to close.

So simply having them on paper isn't good enough. We have to get them in place and get other countries to make the commitments. Thank you, Dr. Adams.

Representative Adams. To follow up on that, what impact would prioritization of rural broadband have on closing this divide?

Ambassador Holleyman. Well, rural broadband is a key part of it to, one, make sure that every citizen in the U.S. economy can build not only their domestic and national and their local engagement, but for those individual entrepreneurs and creators who want to have markets outside of their local community, outside of this country, these are the rules that we need to do it.

That is why President Obama, Ambassador Forman, we believe so strongly in these Digital 2 Dozen provisions because we believe that added to better broadband in the United States, it would create a more equal playing field for all types of American citizens in the fastest growing global markets.

Representative Adams. Thank you. I am concerned by the FCC's repeal of net neutrality allowing internet providers to charge more for certain content or give preferential treatment to certain websites.

So what kind of impact could the FCC's action have on ensuring free digital trade?

Ambassador Holleyman. Well, it is a model that will get picked up by other countries that could increase the disparities in what it costs for people to use the internet.

Generally, in the trade arena, we were trying to find ways to break down barriers. And we believe, again, it is not a technology issue; it is an issue for all economy. And we believe that citizens at every level needed to be able to access. So it is what we are driving in Digital 2 Dozen.

Representative Adams. Ms. Fefer, you stated that China has been persistent in stealing intellectual property.

What are better alternatives for the U.S. to pursue to combat this practice in the digital trade regime?

Ms. Fefer. In order to deal with China, we have various bilateral communication forums that we use to engage with them. It is also an opportunity for the United States to engage with its allies, such as the EU and Japan and others, who have concerns with China's internet sovereignty regime in terms of their cybersecurity law and others, to pressure China to make some changes to it.

I know, Congress is working currently on—the CFIUS reform is working its way through Congress. There are multiple opportunities for engagement with China to explain how their rules can also have a negative impact on domestic Chinese companies in addition to the U.S.——

Representative Adams. Thank you very much. I am out of time.

Mr. Chairman, I yield back.

Chairman Paulsen. Thank you, Dr. Adams.

Representative Handel, you are recognized for 5 minutes.

Representative Handel. Thank you, Mr. Chairman.

And thank you to each of you for being here.

I wanted to stay on the topic of China and the internet sovereignty issue. And Mr. Heather, I wondered if you had any additional insights or comments on that topic. And the same for Mr. Radia.

Mr. Heather. No, I would agree with what was previously stated that, you know, China's approach to sovereignty of the internet is one that is counter to the way in which we look at the internet and its role, not only for digital trade but for speech.

In terms of kind of bridging the question that was previously asked, I would totally agree: The only way to approach China is with our partners around the world. There is no easy fix to our trade problems that we have with the Chinese, but if we don't have partners in those conversations, the job is much tougher.

Representative Handel. Got it.

Mr. Radia, anything to add?

Mr. Radia. I would agree with what Mr. Heather said and echo that the Chinese approach to intellectual property, the censorship of the internet, among other areas, is very problematic, which raises a difficult question in some cases for U.S. internet companies as to whether to engage with China or not in terms of being located in the country and doing business there.

I don't think there is a clear answer to that question universally because, in some cases, engaging and abiding by problematic censorship rules is a better approach. Although some internet companies have decided that they would rather not operate in the country, although users in China can sometimes access their services by circumventing the great firewall of China.

Representative Handel. Thank you. In the Sixth District of Georgia that I represent, we have a fairly significant footprint of Chinese companies based in the district. So, you know, I just wonder ultimately with that approach it is going to eventually come back around and be detrimental to their own companies as well as being detrimental to the U.S.

We are live-streaming this, and it struck me as I was listening to all of the testimony, that we might have some viewers and individuals who are newer to this issue, like I am. And I would be curious to understand sort of the process, because the GDPR was a long time in the making, and sort of how we got to this place. And what was the role of the United States in those negotiations? And did we weigh in, and were our concerns voiced? Were they taken into consideration?

And perhaps, Mr. Heather, you can weigh in, and Ambassador Holleyman.

Mr. Heather. It was a long road to get where we are today. In short, the previous legal framework was developed in 1995, I believe, within the EU. They embarked on an effort to update that. And somewhere along the way Edward Snowden and revelations

associated with NSA came about and put an accelerant into the mix that really limited the ability for the United States Government or the U.S. business community, for that matter, to engage in a way that we might otherwise have been more productive in steering. So there was a bit of a storm of unseen events that occurred that really limited the ability to have effective influence.

Representative Handel. Ambassador.

Ambassador Holleyman. I agree with everything that Mr. Heather said. I mean, the world sort of changed very much after the Snowden leaks in terms of other countries basically not trusting the United States. What I think we have is two opportunities. You know, and we did engage, certainly on the GDPR. It was clear that something was going to happen.

I think we have two options. You know, one is to find these ways that we can be interoperable, which again is to drive the APEC framework. And the challenge that the U.S. has, quite frankly, is that we don't have a uniform privacy law in the United States. Congress has grappled with this for many years.

We have a series of laws that protect health data, other data. And so when you stand that up, quite frankly, against a comprehensive privacy law, it has been through multiple administrations difficult to say, "Adopt the U.S. approach," with a series of different laws. And so the more comprehensive approach of the GDPR is the one that is gaining authority.

So I think as Congress looks ahead, it has been debated, you may want to continue to think, is there a comprehensive framework for the U.S.? And then make sure where we are a player, like APEC, that those end up being truly interoperable and bringing that up to the EU, that we need to make sure that those are interoperable.

Representative Handel. Great. Thank you.

Mr. Chairman, I yield back.

Chairman Paulsen. Thank you.

And, Senator Klobuchar, I recognize you for 5 minutes.

Senator Klobuchar. Thank you very much, Mr. Chairman. Thank you to all of you. This is such an important topic, digital trade, with 95 percent of our potential customers outside of our borders. And I have seen from small businesses in our State that this is the way that they actually get to engage in export that they might not have done otherwise before we had digital trade. In our State, exports were over $20 billion in 2017, and manufacturing accounted for $19 billion of those exports.

So I am starting with one thing that is not manufacturing, and that is tourism. I am the co-chair of the Senate Travel and Tourism Caucus. And we have been doing with Brand USA a lot of advertising digitally of our country.

And, Mr. Heather, can you talk about how digital trade can benefit the U.S. tourism industry in general?

Mr. Heather. I don't think anybody books a flight or an adventure without using the internet these days. So, as I said in my testimony, most of what happens in services trade is now available because of the internet. And we have barely tapped the ability to export our services.

In my opening testimony, I said that only 3 percent of all our services output is exported. So the more that we can facilitate the

movement of data across borders, the more that we can have an open internet system where tourists from outside the United States can see what destinations they can visit in the great State of Minnesota, the better chance there is for there to be tourism in your great State.

Senator Klobuchar. Exactly. And the international tourists spend an average of $4,400 every time they come to our country. So it is more than just the airline business. It is more than the hotel business. It is retail and everything with it.

Reliable data, Senator Capito and I just passed our bill out of the Commerce Committee this morning on getting better measurements for economic impact of broadband along with Senator Sullivan.

And what we are seeing now is that if we don't have that broadband deployed in rural areas, we are not even going to be able to use the equipment that we have or that other parts of the world are using that have better internet in places like Canada or even Iceland.

So could you talk about the importance of that with our modern day machinery and technology?

Mr. Heather. Well, certainly, the ability for any American to access the modern economy requires access to the internet. And innovation doesn't only happen in Silicon Valley. And so the ability to bring real broadband across America so that Americans, wherever they are, have the ability to be entrepreneurs and start up a business, and not only reach other consumers across the U.S., but to those 95 percent of the consumers that exist outside the United States, it is an opportunity to export.

Senator Klobuchar. Thank you.

Ambassador, over the last few years, online companies, as you know, have had some major issues with the disclosure of personal information. And while we know that there is this great advantage of using the internet to improve our economy, and we have some of the world's best companies that have developed these products, coming with it are some issues.

And one of them is this data being disclosed. And Senator Kennedy and I have introduced a bill that is basically a consumer rights bill to improve consumers' protections and online data. As you know, other countries around the world have done this to some success, to some not. But this idea that we have no rules in place at all while we see this increase in digital trade and digital business I think is a real problem. And even Mark Zuckerberg at our hearing told me he thought publicly that we were probably going to have to have some legislation come through Congress.

One of the provisions of our bill he agreed to is a 72-hour limit on notice when a consumer finds out that their data has been breached.

Could you talk about the importance of allowing consumers as part of this move to greater digital trade to allow them to have greater control of their personal data?

Ambassador Holleyman. Senator Klobuchar, I want to thank you. Thank you for the question.

I think the focus on what consumers need and ensuring that there is the right privacy protection and the right tools to address when there are breaches is critical.

I mean, trust in the internet is critical. What we do globally around our trade frameworks like the Digital 2 Dozen, they require countries to have privacy frameworks in place. They don't say exactly what they need to be. It is probably not one size fits all. But, quite frankly, the U.S. should lead on this.

Senator Klobuchar. Well, that has not been happening.

And when we talk on digital trade or transfers of data, we also need to be simultaneously saying, "and we want to do that in a way that protects personal privacy."

So it is not one or the other, transfer data or protect privacy. It should be both. And we should be bold in how we talk about both. So thank you for your question.

Senator Klobuchar. All right. Thank you very much.

Thank you, Mr. Chairman.

Chairman Paulsen. Representative LaHood, you are recognized for 5 minutes.

Representative LaHood. Thank you, Mr. Chairman.

I want to welcome our witnesses here today. Nice to have a fellow Illinoisan on our panel.

Mr. Heather, welcome.

I want to focus first on China and cloud services and access. And as I look at the barriers and hurdles and restrictions that the Chinese have put in place with cloud in particular and whether it is Amazon or Google or Facebook, trying to wrap my arms around how we remedy this situation.

If you look at Alibaba, and you look at their access in the United States, and when you hear the stories of companies that go to China and try to engage in cloud and really the extortion—or fill in your adjective on what you want to use—in terms of what they put in place in terms of that. You know, it is trying to figure out, what is the remedy for that? What should we be doing? You know, trying to work within the framework of international norms on this, but it is extremely frustrating to have that, again, those barriers in place there.

Ambassador, if you could comment on that?

Ambassador Holleyman. Mr. LaHood, you state the problem precisely. And the consequences of what China is doing can't be overstated. I mean, essentially, they are taking away the ability to access their market; they are limiting the amount of access by foreign players. Everything is moving to the cloud, as the CRS report and ITC report note. And if we don't have full access to the market, that will be a long-term hindrance to our companies working globally.

So we were trying to negotiate in the Obama Administration a bilateral investment treaty with China. One of the things we made absolutely clear was that to ever have an agreement with the U.S., we had to have openness in areas like cloud computing. So we need to pursue this at every course.

Secondly, we need allies in this effort. I mean, the TPP partners agree with us on this. They don't want to see Chinese companies

hold this. And so we need to tackle it bilaterally. But, quite frankly, we need friends.

And this is an area where there should be friends because my concern is this: One is that China is the largest market in the world. It will remain the largest market. If Chinese companies, many of whom have fine products, like an Alibaba, if they have a protected market in China and then can access the rest of the world, U.S. companies can access the rest of the world but not China, then that is not only distortive to the economy, but in areas like data analytics, AI, where you need information, for non-Chinese companies to essentially have none of that information is not only economically harmful, but it decreases their efficiency long term. And that is why the barrier is bad today and is getting worse over time.

Representative LaHood. Thank you for that. I do want to switch to another topic here.

Just broadly on trade. And Mr. Heather, I will ask you this. You know, I look at kind of this, what I would describe protectionist path that this is headed down, whether you look at TPP, whether you look at NAFTA, whether you look at steel and aluminum. And particularly in the NAFTA negotiations, I look at the collateral damage that will be done to digital trade and other things by what I would call unconventional and unorthodox positions that we have taken in NAFTA negotiations.

Look at ISTS. Look at sunset provision. Look at rules of origin. You know, these are, I think, hurdles, barriers, that are really, really hard to get our partners to agree upon.

Can you comment on that on whether you are optimistic with the approach we have taken, that we are going to reach a resolution on this?

Mr. Heather. First of all, it is good to see you. You probably don't remember, but 21 years ago, I worked for Lolita Didrikson, and we met in that capacity.

Representative LaHood. Yep.

Mr. Heather. I was thinner then and had more hair, but anyway, it is good to see you.

I think you have painted the problem accurately. If we are going to confront China, we need partners. And the activity that this Administration and the agenda that this Administration has pursued has kind of poked the eyes of all the partners that we need to be aligned with us in conversations with China.

And from that standpoint, at least in the immediate near future, I don't have a lot of hope for having a dialogue with China that will involve the EU, will involve Japan, will involve Canada, will involve the collection of TPP countries that we used to be aligned with in having a whole-of-country approach, global approach to addressing the concerns with China.

At some point, I suspect that will change, but at least in the short term, the actions that this Administration have taken have not created an environment for us to find partners.

Representative LaHood. Thank you. Thank you, Mr. Chairman. Thank you.

Chairman Paulsen. Thank you. And I want to thank all of the witnesses for being here.

I think you could see from the engagement on both sides of the aisle, there is a recognition that there is potential, huge potential, and opportunity for where the United States can go and should go and needs to go in this space.

And so I think that your comments across the board have reinforced that, and we have some suggestions to follow up on now, actually, and continue to drive attention to this.

So, with that, I want to remind members that should they wish to submit questions for the record, the hearing record will remain open for 5 business days.

And, with that, this hearing is adjourned.

[Whereupon, at 11:12 a.m., the committee was adjourned.]

SUBMISSIONS FOR THE RECORD

I call this hearing to order.

Every day, when Americans sit down to order goods from a website or consume media online, we are participating in a vibrant digital economy—an economy that takes the ideas and creations of artists, manufacturers, and innovators and puts them within reach of our couches and kitchens.

Digital trade means supply chain tracking, 3–D printing, or digital platforms that lead to ecommerce, cloud computing, and social media. You know the names of the leaders in each of these areas: Facebook, Amazon, eBay, and so on. That's because the United States has pioneered this digital revolution.

What many don't realize is that trade in manufactured goods is itself a part of the digital economy. From the websites that market the goods, to the payment processing systems that carry out the transaction, the digital economy facilitates the movement of all kinds of consumer products from warehouses to family homes. American manufacturing relies on E–Commerce and digital trade.

The benefits of digital trade include domestic economic growth as well as spreading American ideas and culture across the world. Of course, to us, this is good. Yet, there are others who consider the free flow of information, products, and ideas a threat to their control.

Nearly three decades after the Berlin Wall fell, the way ideas and goods travel from one nation to another remains a contentious issue, both politically and legally.

In fact, because of the novelty of digitization, commercial principles and freedoms that were carefully developed for conventional trade and gained international consensus are at risk of being circumvented.

With every innovation comes opportunity for economic advancement but also opportunity for some foreign governments to grow their own power. In today's interconnected economy, they can have wide-ranging effects on international commerce and other national economies as well as the free flow of information.

Digital technology does raise legitimate privacy and cybersecurity concerns but some governments may not be sufficiently concerned with the effects of their policies on trade and some may even be using these concerns as an excuse for protectionist and other purposes.

Some foreign governments impose additional taxes and fees, and some governments will only permit sales on the condition of storing data locally or providing the source code that will inevitably be used for a competing, state-backed product.

Some governments that otherwise enforce property and contract laws turn a blind eye to, or even facilitate, intellectual property theft. This is especially true when the division between the State apparatus and the private sector is nonexistent.

Up on the screen right now is a map of the world showing the prevalence of digital trade barriers.

The lighter colored regions like Australia, Canada, and Mexico are perceived to have taken a light-handed approach to trade barriers.

At the other end of the spectrum are trading blocs and countries like the EU and China that make access to their markets far more difficult and costly.

In part, their motivation likely is to catch up to the United States, the leader in digital technology development, and try to take the lead themselves.

American companies have always thrived in a competitive market, but the competition must be fair and free from foreign government intervention on behalf of their domestic companies.

That is why global players with large economies, such as China and the European Union, which represent large global market shares, should see the rewards of developing their own digital economies without discriminatory standards and testing requirements, localization requirements, forced technology transfers, and the like.

Governments with control over market access should not use their leverage to extract concessions from companies in competition with one another.

In the decades after World War II, U.S. companies dealt with smaller economies that saw the likely economic benefit of opening their marketplace. Their citizens benefited from more choice, lower prices, and faster economic growth.

We must be vigilant to preserve the principles that have already led to great prosperity throughout the world in the digital trade arena.

That means addressing, swiftly and clearly, the excessive burdens foreign governments place on American digital products, so that we are not unfairly disadvantaged and can compete on the merits.

That also means negotiating new agreements that protect not just American's economic interests, but allow the free exchange of culture and ideas throughout the world.

The world is a better place thanks to American ideas and commerce. Keeping the global digital marketplace open means continuing the fight for that better world.

Before I introduce our witnesses, I will now yield to Representative Beyer for his opening remarks.

STATEMENT OF HON. DONALD S. BEYER, JR., A U.S. REPRESENTAIVE FROM VIRGINIA
[STANDING IN FOR RANKING MEMBER SENATOR MARTIN HEINRICH]

Thank you Mr. Chairman.

Since this Committee took up digital trade last fall, President Trump's has waded into the trade issue in unpredictable and destabilizing ways.

The President's erratic, aggressive approach is creating an environment of economic uncertainty, is alienating our trading partners and allies, and risks harming the global economy.

So far, the President and his trade advisors have seemed uninterested in the significant majority of the U.S. economy that does not consist of heavy manufacturing.

Not only has digital trade not been front and center, it seems the Administration simply does not have a strategy for how to strengthen U.S. leadership in digital trade, nor any interest in creating one.

Ceding ground to others, including competitors who are putting up new barriers, hurts our economy and our workers.

This failure to lead is a missed opportunity for U.S. small businesses, technology companies, manufacturers and farmers, and all who benefit from the increased export opportunities made possible by digital trade.

It also risks the United States falling behind as other countries race to create the technologies of the future and write rules for operating in the digital economy.

Strengthening our position in digital trade starts right here at home, by ensuring an open internet that enables innovation to flourish.

To that end, it is critical that we restore network neutrality—which is vital for small business owners who rely on the internet to compete with bigger companies.

It also means expanding access.

Too many people still don't have access to a broadband connection. Their ability to compete in an increasingly digital economy is undermined without high-speed internet.

We need to keep our focus on creating opportunities for all Americans.

As we will hear this afternoon, the digital playing field around the globe is far from level.

When dealing with China, American companies confront rampant theft of U.S. intellectual property, forced technology transfer policies, data localization requirements, and other efforts to tilt the playing field against the United States.

Equally concerning, China is becoming a model for other countries who are erecting trading barriers that restrict the free flow of data.

We need to knock down these barriers in a systematic, thoughtful way, rather than pursuing a policy of ill-conceived tariffs that will create additional barriers to trade.

Burdensome data regulations are particularly onerous for small and medium-sized firms that don't have big IT departments or can't absorb the added costs of having to store data locally or comply with other requirements.

Digital trade is just one piece of a broader trade landscape. And in the last few months, it has been harder and harder to understand the Administration's positions on a range of trade issues.

One Wall Street analyst estimates that the Administration's erratic trade policies have cut the value of U.S. equities by about $1.25 trillion.

And the costs extend beyond the stock market.

The Administration's tariffs on solar panels will cause the loss of thousands of jobs and the delay or cancellation of billions of dollars of investments in solar energy. These tariffs will slow our transition to renewable energy.

The Administration has used dubious national security justifications to levy counterproductive tariffs on our closest allies. The President has repeatedly acknowledged that theses tariffs are not justified by national security concerns, undermining any future U.S. case at the WTO.

By levying these tariffs, he has managed to damage our economy and our alliances in one fell swoop.

Of course, the negative aspects of President Trump's trade policy are compounded by his dyspeptic approach to diplomacy. Nowhere was this clearer than his catastrophic performance at the G–7 in Charleroi.

Public expressions of disdain for the leaders of our democratic allies will only make them less likely to engage in productive trade negotiations. As the President becomes increasingly unpopular abroad, it will become more difficult for democratic leaders to enter into new agreements with the United States.

We need a trade policy that is guided by principle, not whim, and that is forward-looking and not reactionary. Something we saw from the previous Administration.

But that's not where we are today. The way President Trump has gone about renegotiating NAFTA has generated instability.

He's fighting almost daily with Canada and his threats to leave the deal risk disrupting markets and raising prices and may trigger retaliatory tariffs.

Rather than pursue productive discussions with China to drive changes in their trade practices, President Trump has launched a trade war, rolling out $50 billion in tariffs and threatening another $200 billion in tariffs last week. China immediately promised retaliatory tariffs of the "same scale."

Even the President's Council of Economic Advisers prepared an internal analysis showing that tariffs will harm our economy.

Trade is often an area ripe for bipartisan agreement and that's especially true in the area of digital trade.

But the damage to trading relationships from the Administration's moves to impose tariffs on steel, aluminum and other products harms the United States' ability to forge partnerships that will expand trade, both online and offline.

And that uncertainty has a chilling effect on trade of all kinds. We have only begun to see the damage from Trump's trade policies.

I look forward to hearing from our witnesses about how we can promote digital trade and knock down barriers and how the Administration can play a more constructive role.

Statement of the U.S. Chamber of Commerce

ON: The Need for U.S. Leadership on Digital Trade

TO: U.S. Congress Joint Economic Committee

BY: Sean Heather
Vice President
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

DATE: June 21, 2018

1615 H Street NW | Washington, DC | 20062

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. The Chamber is dedicated to promoting, protecting, and defending America's free enterprise system.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are also active members. We are therefore cognizant not only of the challenges facing smaller businesses, but also those facing the business community at large.

Besides representing a cross section of the American business community with respect to the number of employees, major classifications of American business—e.g., manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Thank you for inviting the U.S. Chamber of Commerce to testify before this committee. Advancing America's interest in the global digital economy needs to be a top international priority and we need a *whole of government* approach to work with key trading partners to counteract trade and regulatory barriers that adversely impact trade in digital goods and services.

In previous testimony before this committee, I highlighted how the United States has positioned itself as a leader in the global digital economy; however, our advantage is not assured as certain governments are unnecessarily restricting digital commerce and seeking to undermine American technological innovation. Today, many countries are still pursuing a flawed approach to economic development. Restrictions on cross-border data flows via forced localization measures, new complex and burdensome regulatory regimes, irritants *de minims* to e-commerce, investment measures that force technology transfers, and misuse of competition law are some of the most common challenges digital goods and services of American companies of all sizes, across all sectors, face in foreign markets.

The Chamber's desire is that our trading partners would recognize the economic potential of a liberalized approach to digital trade and join the United States in championing trade obligations that support digital trade and work across borders to resolve problematic regulatory frameworks. In order to make more progress, we need a robust agenda that deploys a strategy that takes a *whole of government* approach to our engagement abroad.

Identifying the Problem

Every good strategy starts with understanding the problem. In recent years, we have done a good job of documenting the rising challenges to digital trade. The Office of the United States Trade Representative (USTR) has focused its National Trade Estimate on digitally related concerns in foreign markets.[1] The International Trade Commission is in the process of conducting three studies, the first of these studies released last year outlined some of the main restrictions to digital trade, including data localization, data protection and privacy, cybersecurity, censorship, market access, and investment.[2] The second and third studies will drill down and focus on foreign trade restrictions in the business-to-business and business-to-consumer markets. In May of this year, the Congressional Research Service made its contribution through its report entitled *Digital Trade and U.S. Trade Policy*.[3] Such research efforts should continue, but together these and other contributions have effectively shined a light on the barriers American companies face in delivering digital products and services.

[1] https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital

[2] https://www.usitc.gov/publications/332/pub4716.pdf

[3] https://fas.org/sgp/crs/misc/R44565.pdf

Importance of Services

We need to recognize the importance of services trade to our economy and to the digital economy. Consider:

- **Services Everywhere.** Services dominate the U.S. economy. Broadly speaking, services provide about 80% of all American jobs (approximately 125 million of 156 million American jobs, according to the Bureau of Labor Statistics).

- **More Jobs, Higher Pay.** Professional and business services employ 20.8 million Americans, making this sector a larger employer than manufacturing (66% larger, in fact). What's more, these are good jobs with average hourly earnings of $32.

- **Increasingly Tradeable.** Many services can be exported, particularly those categorized broadly as professional and business services. These include fields such as audiovisual, software, architecture, accounting, engineering, project management, banking, insurance, waste management, and advertising. The Internet is making more of these services tradeable every day.

- **Competitive Advantage.** The United States has become the world's largest exporter of services. U.S. service exports reached $777.9 billion in 2017, and the United States has a trade surplus in services of nearly $250 billion. Services sales by foreign affiliates of U.S. multinational corporations top $1.4 trillion.

- **Untapped Potential.** Despite these big numbers, the potential for service industries to engage in international trade is almost untapped. One in four U.S. factories export, but just one in every 20 providers of business services does so. Just 3% of U.S. services output is exported, according to the Peterson Institute for International Economics.

Without question, trade in manufactured products is very much a part of the digital economy. Whether simply sold through e-commerce channels or part of the growing numbers of products that make up the Internet of Things, American manufacturing is at the heart of the digital economy. However, we must not overlook our dominant position in trade in digital services. The United States enjoys a tremendous trade surplus in services and service jobs are some of the most well paid jobs in our economy. Therefore, our engagement abroad in support of digital trade must start with our support for our service industries that underpin all things digital.

Developing Expertise and Capacity to Engage

Both the State Department and the Department of Commerce play an important leadership role in digital trade. Our foreign embassies are the first line of defense against impediments to digital trade and are important messengers for a liberalized approach to the digital economy. The Bureau of Economic and Business Affairs at State plays a central role in coordinating U.S. engagement internationally on ICT and cyber policy matters, but also serves as an active voice in support of digital trade.

The Department of Commerce plays a critical role in advancing U.S. digital exports, and advocating for the adoption of U.S.-friendly digital regulatory frameworks. It also has a core responsibility to internationally safeguard the voluntary-private sector approach to standards development that underpins many ICT products.

Since its inception in 2016, working with the State Department, the Commerce Department has operated a Digital Attaché Program that has proven to be a valuable resource through which U.S. stakeholders can identify, respond to, and avert policies that would otherwise have been harmful to the competitiveness of U.S. businesses. This program trains and embeds U.S. digital policy experts in the U.S. embassies of our key trading partners. Expanding this program, ensuring adequate resources, and giving digital attaches a clear mandate focused on digital trade is critical to ensuring American leadership in the digital economy. Foreign governments are deploying substantial resources to promote digital trade rules that benefit their own businesses and simultaneously erode U.S. digital competitiveness. This includes robust promotion of their privacy frameworks, overwhelming participation in standard setting bodies, and the use of cybersecurity laws to promote industrial policies. We strongly encourage the U.S. Department of Commerce to expand the number of Digital Attachés that are based around the world and ensure that they are adequately resourced to fulfill their role.

Data Flow Agreements

The U.S. government should do more to support international privacy and cybersecurity frameworks that facilitate digital trade and the seamless movement of data across borders. The United States needs to maintain the EU-U.S. Privacy Shield. That agreement is important to data flows for both Europe and the United States. We applaud the Administration for its efforts last year that ensured the agreement successfully made it through its first annual review and the business community looks forward to supporting the review this year post Europe's GDPR implementation.

While Privacy Shield represents one framework for moving data across borders, it should not be viewed as the only model. The United States has importantly also advanced, within APEC, the Cross Border Privacy Rules (CBPRs) that promote the movement of data between borders to bridge national privacy regimes. The United States and other governments that have adopted the CBPRs should do more to encourage other APEC governments to join. Further, it is important that the United States develop similar mechanisms within other regions such as Latin America and other non-EU, non-APEC countries.

While difference between privacy regimes can be bridged through these mechanisms, increasingly cybersecurity regulatory frameworks are being developed that also threaten the movement of data. The United States has created the NIST Framework for Improving Critical Infrastructure Cybersecurity, an innovation-friendly framework encouraging technology-neutral approaches to managing cyber risks. However, approaches being developed in foreign jurisdictions often look much different. The United States needs to become more active in both shaping and aligning these emerging regulations, but also developing new mutual recognition agreements to address cross-border cybersecurity requirements, similar to what have been

achieved to ensure data movement in relationship to national privacy regimes. In doing so, improved coordination among cybersecurity regulations will not only facilitate digital trade, but will also increase levels of cybersecurity by enabling companies to scale best-in-class cyber solutions across borders.

Developing Digital Trade Rules

The United States should continue to write global digital trade rules in our bilateral and multilateral agreements. The Chamber sees the need to seek commitments from our trading partners to support digital trade in goods and services and foster the cross-border movement of data. The U.S. government should prioritize digital issues in its trade agenda and ensure they receive sustained, high-level attention by the USTR and other relevant agencies.

We welcome USTR's efforts to modernize the North American Free Trade Agreement (NAFTA) to include important digital trade provisions. We also strongly support the United States playing a leading role within the World Trade Organization (WTO), which this year has undertaken important efforts among 70 countries to develop e-commerce rules that ensure an open and predictable marketplace for American businesses.

We would also encourage the Administration to consider relaunching negotiations around the Trade in Services Agreement (TiSA). TiSA has the potential to be more than just a "services" agreement as it could provide data flow commitments to the benefit of all industries across all sectors. It also, unlike the efforts underway within the WTO, is a negotiation that would extend digital trade commitments beyond e-commerce, and given the smaller number of countries involved in the negotiation, TiSA represents an opportunity to potentially reach a higher-standard agreement.

G7/G20 Engagement

The G7 and G20 are important venues for shaping the agenda for several of the world's leading governments as they each seek to make policy decisions affecting the digital economy, which then directly impacts digital trade. In recent meetings, the G7 and G20 have placed an emphasis on the digital economy as part of its conversations. The United States has worked hard to ensure G7 and G20 digital communiques carry the right messages on regulation, combating protectionism, and the benefits productive engagement with the digital economy holds for every nation.

However, behind the scenes it has been increasingly more difficult to maintain positive statements related to the digital economy as certain members seek to advance alternative agendas. We would recommend that the United States identify G7 and G20 partners across a range of digital policy matters and then work with these select partners well in advance of future meetings to develop strong common positions on these issues. Without more forward planning, we fear that the digital policy discussions in the G7 and the G20 may reach a stand still.

Role for Regulators

While USTR, Commerce, and State play focal point roles in developing and advocating the U.S. digital trade strategy, U.S. regulators are very much needed for a *whole of government* approach to be effective. The Federal Trade Commission has been active with Department of Commerce to advance abroad an understanding of U.S. privacy protections, in shaping foreign privacy laws, and in being the enforcement behind data flow agreements like the EU-U.S. Privacy Shield.

Other U.S. regulators are also increasingly being relied upon to answer the call. U.S. financial regulators need to take on a leadership role to ensure regulatory frameworks abroad don't limit opportunities for U.S. fintech leadership. But to do so, the U.S. must overcome our fragmented banking regulatory structure, perhaps by turning to the Financial Stability Oversight Council as a convening body to ensure that U.S. regulators are on the same page. U.S. auto and aviation regulators also need to engage internationally to shape foreign counterparts' regulatory designs that will affect American competitiveness abroad for autonomous vehicles and drones. Further, regulators in foreign markets are beginning to contemplate regulatory questions about artificial intelligence, machine-based decision making, access to algorithms and big data, as well as a host of other issues. In short, a *whole of government* approach requires the entire U.S. government to be vigilant, coordinated, and better prepared to actively work to shape foreign regulatory environments that will deeply impact American companies' ability to innovate and compete in foreign markets.

Conclusion

The Chamber is pleased to offer this testimony. The Chamber and its members look forward to engaging with the Congress and the Administration to enhance existing efforts to drive better policy outcomes in cooperation with our key trading partners to advance digital trade to the benefit of American companies, workers, and our economy, but also for the benefit of the partner economies our members serve.

Testimony of Ryan Radia
Research Fellow & Regulatory Counsel
Competitive Enterprise Institute

Before the Joint Economic Committee of the United States Congress

Hearing: The Need for U.S. Leadership on Digital Trade

June 21, 2018

Chairman Paulsen, Ranking Member Heinrich, and Members of the Committee, thank you for giving me the opportunity to testify before you today. My name is Ryan Radia. I am research fellow and regulatory counsel at the Competitive Enterprise Institute (CEI),[1] where I focus on adapting law and public policy to the unique challenges of the information age. CEI is a nonprofit, nonpartisan public interest organization dedicated to the principles of limited constitutional government and free enterprise. CEI has supported trade liberalization through analysis and advocacy for over 25 years.[2]

At this critical juncture for international trade and Internet commerce, the United States must maintain its historic role as the global leader in efforts to promote free trade and open markets. This leadership is especially important in the information economy. In the U.S. technology sector, half a million businesses collectively employ over 11 million Americans and generate $1.6 trillion in annual economic output.[3] This sector's global reach is extensive: U.S. tech firms export over $300 billion annually in products and services, supporting over 800,000 American jobs.[4] Therefore, it should, come as no surprise that public policies inhibiting the unfettered flow of digital services between the United States and the rest of the world threaten consumers, workers, and innovation.

---

1. *See, e.g.*, James M. Sheehan, *Two Years after NAFTA: A Free Market Critique and Assessment* (Competitive Enter. Inst. 1995), https://cei.org/studies-issue-analysis/two-years-after-nafta-free-market-critique-and-assessment; Matthew C. Hoffman, *Walking Through NAFTA: A Critical Examination of the North American Free Trade Agreement*, Competitive Enterprise Institute, 1993. CEI has also joined with free-market organizations in recent years to emphasize the importance of free trade to American prosperity. Coalition Letter, *Open Letter to Congress: Free Trade Is Essential to American Prosperity*, September 22, 2016, https://cei.org/sites/default/files/L16%2009-22%20Trade%20Coalition.pdf.
2. My biography and writings are https://cei.org/expert/ryan-radia. Wade Burkholder, CEI Research Associate, assisted with the preparation of this testimony.
3. CompTIA, *Cyberstates 2018: The Definitive National, State, and City Analysis of the U.S. Tech Industry and Tech Workforce*, at 9–11 (2018), https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2018.pdf.
4. CompTIA Tech Trade Snapshot, *Imports and Exports of Tech Products and Services*, at 1 (May 2018), http://tradepartnership.com/wp-content/uploads/2018/05/CompTIA-Tech-Trade-Snapshot-2018FINAL1.pdf.

Tariffs and non-tariff barriers to trade can and do undermine free trade in the digital marketplace. In my testimony, I wish to focus on another set of policies that threaten digital trade: governmental regulations regarding privacy, copyright, and antitrust. Of particular importance in the regulatory arena is the European Union (EU), whose member states collectively represent America's single largest trading partner in goods and services.[5] EU residents play an especially influential role in the information economy, with roughly 430 million Internet users residing in EU member states.[6] As such, Facebook has more European users than American users,[7] while Google's popularity as a search engine among Europeans exceeds that among Americans.[8]

Although most major U.S. technology companies consider EU residents to be a core aspect of their user bases, the European Union's approach to regulating the information economy differs from the approach of U.S. policymakers, in some cases dramatically. A complete overview of EU regulation of the technology sector is beyond the scope of my testimony, but I wish to focus on three areas of EU regulation that pose a particularly large threat to the free flow of digital goods and services between the United States and the European Union: (1) privacy; (2) copyright; and (3) antitrust.

EU Privacy Regulation and U.S. Internet Companies

On May 25, 2018, the EU's General Data Protection Regulation (GDPR) entered into force, marking perhaps the most significant policy change in EU history regarding how data collection is regulated.[9] The GDPR applies to any company that processes or controls data on EU "data subjects," no matter where the company is domiciled or has a physical presence.[10] The GDPR purports to affirm "digital rights" for EU persons by requiring companies to, among other things, provide users all their data in a machine-readable format and delete a user's data at his or her request.[11] While the GDPR does not distinguish between online and offline data collection, high-tech and financial services companies will bear the brunt of complying with the regulation.[12]

---

5. U.S. trade in goods and services with the European Union totaled $1.16 trillion in 2017, including $528 billion in exports and $629 billion in imports. *See* U.S. Census Bureau and U.S. Bureau of Economic Analysis, *Monthly U.S. International Trade in Goods and Services, April 2018*, at 26 (June 6, 2018), https://www.census.gov/foreign-trade/Press-Release/current_press_release/ft900.pdf.

6. Of the approximately 510 million residents of EU households, 85 percent have Internet access. Eurostat, *Internet access and use statistics - households and individuals*, 2016, https://goo.gl/bxKV9P.

7. David Ingram, "Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law," Reuters (Apr. 18, 2018), https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P.

8. Robinson Meyer, "Europeans Use Google Way, Way More than Americans Do," *The Atlantic* (Apr. 15, 2015), https://www.theatlantic.com/technology/archive/2015/04/europeans-use-google-way-way-more-than-americans-do/390612/.

9. EU General Data Protection Regulation (in effect on May 25, 2018), https://gdpr-info.eu/.

10. *See* GDPR ch. 1, art. 3.

11. *See id.* ch. 3, arts. 17–20.

12. Ryan Radia & Ryan Khurana, "European Union's General Data Protection Regulation and Lessons for U.S. Privacy Policy," *OnPoint* No. 245, Competitive Enterprise Institute, May 23, 2018, https://cei.org/content/european-unions-general-data-protection-regulation-and-lessons-us-privacy-policy.

The GDPR entered into force less than one month ago, but the regulation has already resulted in several notable changes for Internet users in the EU and around the world. The recent onslaught of privacy policy updates and mass emails from Internet companies is perhaps the most widespread result of the GDPR's implementation.[13]

Yet, the regulation's less noticeable implications for Internet users may well prove to be far more significant in the long run. In particular, the GDPR has changed how many companies, including U.S. companies, interact with EU users—and, in some cases, all of their users. Failing to comply with the GDPR may entail a fine of up to €20 million ($23.16 million) or 4 percent of a firm's global revenue, whichever is greater.[14] This risk, along with the uncertainty surrounding many of the regulation's provisions, has led many U.S. firms to simply stop allowing EU subjects to access their platforms and services.

For instance, the major American media company Tronc (formerly Tribune Publishing), which owns major news outlets including the *Chicago Tribune*, *Los Angeles Times*, *New York Daily News*, and *Baltimore Sun*, began blocking access to European users almost immediately after the GDPR entered into force.[15] A&E Networks, which owns several television channels, followed suit.[16] Even several firms outside the United States—such as Ragnarok Online, a South Korean massively multiplayer online role-playing game—have also responded to the GDPR by blocking European users.[17]

Some firms responded to the GDPR's implementation by shuttering their doors entirely. For instance, Klout, an Internet analytics firm that enabled thinkfluencers to gauge the effectiveness of their social media presence ("nextification"), ceased operations on May 25, 2018, the day the GDPR became effective.[18] And the GDPR has resulted in several independent American video game developers temporarily or permanently shutting down their Internet gaming platforms in EU member states.[19]

---

13. J.D. Biersdorfer, "Why All the New Terms of Service?" *New York Times*, April 30, 2018, https://www.nytimes.com/2018/04/30/technology/personaltech/why-all-the-new-terms-of-service.html.

14. GPDR, ch. 8, art. 83.

15. Adam Satariano, "U.S. News Outlets Block European Readers over New Privacy Rules," *New York Times*, May 25, 2015, https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html.

16. *Id.*

17. Emma Kidwell, "Ragnarok Online Shutting down European Servers after 14 Years," Gamasutra, April 25, 2018, https://www.gamasutra.com/view/news/317050/Ragnarok_Online_shutting_down_European_servers_after_14_years.php.

18. Will Oremus, "Klout Is Shutting Down Just In Time to Not Reveal How Much It Knew about Us," Slate, May 10, 2018, https://slate.com/technology/2018/05/klout-is-dead-just-in-time-of-europes-gdpr-privacy-law-thats-not-a-coincidence.html; *see also generally* https://twitter.com/ProfJeffJarviss [last visited June 18, 2018].

19. *See, e.g.*, Alice O'Connor, "Loadout Shutting down this Month ahead of GDPR," Rock Paper Shotgun, May 9, 2018, https://www.rockpapershotgun.com/2018/05/09/loadout-shutting-down-because-of-gdpr/; IO Interactive, "Hitman Absolution Service Message," accessed June 20, 2018, https://www.ioi.dk/hitman-absolution-service-message/.

As EU member states implement local GDPR laws and begin to bring enforcement actions, the GDPR may ultimately result in U.S. firms erecting digital walls to deny access to EU residents on an unprecedented scale.[20] This disruption in digital trade risks not only denying EU residents the benefits of accessing American platforms and content, but also depriving U.S. firms of revenues generated from serving European users. This may in turn hurt U.S. consumers: many tech firms can deliver their services at a trivial marginal cost, but a declining user base means there will be fewer customers from which tech firms are able to recoup their high fixed costs.[21] Consumer choice will suffer as a result, especially if firms find that it no longer makes economic sense to offer advertiser-supported content and services.

Many U.S. firms will continue serving EU subjects in spite of the GDPR's implementation, to be sure. Because the GDPR requires firms to obtain express consent from EU users before using their data for the purpose of delivering individualized advertising, however, the millions of Europeans who have grown accustomed to accessing U.S. platforms and services at no monetary cost may soon end up paying out of pocket for products they traditionally considered to be "free." For instance, *The Washington Post* recently began offering a "Premium EU Subscription" to users who decline to consent to the company sharing their information with third parties.[22] This subscription costs 50 percent more than the *Post*'s traditional online subscription, which includes personalized ads.[23] Some EU residents might prefer to pay for ad-free subscriptions in any event, but to the extent that such business models make sense, several companies offer them already.

For U.S. firms that elect to comply with the GDPR's mandates, the ensuing costs could be significant. According to estimates from EY (formerly Ernst & Young) and the International Association of Privacy Professionals, the average Fortune 500 company has spent $16 million to comply with the GDPR over the past two years.[24] Brian Donohue, head of Pinterest's Instapaper unit, wrote in April 2018 that he "underestimated the scope of work and it was not possible to complete by the deadline, this was the required alternative."[25]

---

20. Just before the GDPR's implementation date, only seven of the EU's 28 member states had passed GDPR implementation acts. David Meyer, "Most Member States Won't Be Ready for GDPR," The Privacy Advisor, International Association of Privacy Professionals, April 24, 2018, https://iapp.org/news/a/most-member-states-wont-be-ready-for-gdpr/.

21. Ronald Coase, a Nobel Prize-winning economist, discussed the political challenges entailed in regulating information-age industries characterized by declining marginal costs in a 2004 interview with CEI founder Fred L. Smith, Jr. Competitive Enterprise Institute, *Declining Marginal Cost Industries in the Global Information Age* (CEI Event, May 7, 2004), http://www.cei.org/pdf/DMC_transcript.pdf.

22. Lucia Moses, "The Washington Post Puts a Price on Data Privacy in its GDPR Response — and Tests Requirements," Digiday (May 30, 2018), https://digiday.com/media/washington-post-puts-price-data-privacy-gdpr-response-tests-requirements/.

23. *Id.*

24. *See* Mehreen Khan, "Companies Face High Cost to Meet New EU Data Protection Rules," *Financial Times*, November 19, 2017, https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.

25. "GDPR: Tech Firms Struggle with EU's New Privacy Rules," BBC News, May 24, 2018, https://www.bbc.com/news/technology-44239126.

Compliance costs may grow larger still as EU member states enact GDPR legislation in the coming years, especially if ambiguities in the regulation are clarified to extend its scope to U.S. firms that control or process EU user data to a limited extent. For instance, GDPR Article 27 provides that firms are not required to hire a data protection officer if their processing of data on EU subjects is "occasional" and "does not include, on a large scale, processing of special categories of data."[26] Because defining the terms "occasional" and "large scale" is up to EU member states, even small U.S. firms that handle a relatively limited volume of data on EU residents may end up subject to the full brunt of the GDPR's mandates. Time will tell.

The GDPR also has implications for competition and entry into the global information economy, in which U.S. firms have been the most successful globally to date. As many commentators have noted, under the GDPR, companies that operate platforms with high worldwide adoption will likely benefit from the regulation. Major technology businesses such as Facebook and Google already employ and retain extensive teams of lawyers, privacy professionals, and engineers. Their would-be rivals, in contrast, face substantial capital constraints regarding compliance costs.

Whereas Facebook and Google were able to upset once-powerful incumbents such as Myspace and Yahoo! on a relatively modest budget, tomorrow's innovators with brilliant new ideas may struggle to unseat today's incumbents due to regulations such as the GDPR that did not exist 15 or 20 years ago.[27] According to a recent report in *The Wall Street Journal*, addressing the GDPR's imminent implementation, "[s]ome advertisers are planning to shift money away from smaller providers and toward Google and Facebook."[28] And as *The New York Times* recently reported, major developing countries such as Brazil and Argentina are considering privacy regulations based on the European approach.[29]

Regardless of one's views on how governments should regulate how consumer data is used, shared, and protected, the GDPR will undoubtedly have a significant effect on the flow of digital trade between the United States and the European Union. As the U.S. Senate and House of Representatives consider enacting domestic privacy legislation,[30] U.S. lawmakers should carefully

---

26. GDPR ch. 4, art. 27.

27. Adam Thierer, How Well-Intentioned Privacy Regulation Could Boost Market Power of Facebook and Google, Technology Liberation Front, April 25, 2018, https://techliberation.com/2018/04/25/how-well-intentioned-privacy-regulation-could-boost-market-power-of-facebook-google/.

28. Sam Schechner & Nick Kostov, "Google and Facebook Likely to Benefit from Europe's Privacy Crackdown," *Wall Street Journal*, April 23, 2018, https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.

29. Daisuke Wakabayashi and Adam Satariano, "How Facebook and Google Could Benefit from the G.D.P.R., Europe's New Privacy Law," *New York Times*, April 23, 2018, https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html.

30. *See, e.g.*, Balancing the Rights of Web Surfers Equally and Responsibly Act (BROWSER) Act, H.R. 2520, 115th Congress, 2017; Social Media Privacy and Consumer Rights Act of 2018, S. 2728, 115th Congress 2018; Customer Online Notification for Stopping Edge-Provider Network Transgressions (CONSENT) Act, S. 2639, 115th Congress, 2018.

examine the repercussions of the GDPR, including its effects on small businesses, market entry, and business models that depend on personalized advertising.

Instead of mimicking the EU's privacy regime or seeking to impose even more stringent rules on tech companies, it is imperative that American policymakers consider the tradeoffs that restricting data collection would entail for consumers. Reshaping the information economy through privacy regulation may come at a steep price. Just as U.S. leadership has helped steer the world toward freer trade and open markets, the United States should lead by example on privacy, and resist calls to adopt an overly precautionary approach that might endanger the freedoms that have enabled U.S. firms to connect the world through platforms that can help improve the lives of billions of people.[31]

EU Digital Single Market and U.S. Creative Works

EU residents, like consumers worldwide, regularly watch movies, television shows, and streaming video content. The U.S. continues to lead the world in its creative industries, including not only Hollywood's venerable film studios,[32] but also America's television and streaming video companies.[33] These companies distribute their content through a diverse array of business models, reflecting consumers' growing preference for watching video programming over streaming Internet platforms.

The EU has long pursued regulations governing how content owners make their programming available in various ways to EU residents of different member states.[34] Existing EU regulations require content providers to allow EU consumers who have purchased content in their home country to allow those consumers to access that content while traveling elsewhere within the EU on the same terms as if they were still in their home country.[35]

---

31. For a discussion of the precautionary principle and privacy, see Adam Thierer, "Privacy Law's Precautionary Principle Problem," *Maine Law Review*, Vol. 66, No. 2 (2014), pp. 471–476, https://www.mercatus.org/system/files/05-Thierer.pdf.

32. Although film studios based outside the United States have enjoyed growing revenues and output in recent years, Hollywood's major film studios and their partners continue to generate the lion's share of the global box office. *See, e.g.*, Michael Cieply, "Hollywood Works to Maintain Its World Dominance," *New York Times*, November 3, 2014, https://www.nytimes.com/2014/11/04/business/media/hollywood-works-to-maintain-its-world-dominance.html; Phil Hoad, "Hollywood's Hold Over Global Box Office—63% and Falling," *The Guardian*, April 2, 2013, https://www.theguardian.com/film/filmblog/2013/apr/02/hollywood-hold-global-box-office.

33. For a discussion of U.S. streaming video platforms' global dominance, see Reinhardt Krause, "Netflix Takes on Media Giants as Video Streaming War Goes Global," *Investor's Business Daily*, March 8, 2018, https://www.investors.com/research/industry-snapshot/netflix-fights-media-giants-in-global-video-streaming-war/.

34. *Cf.* Regulation 2018/302, which encompasses non-audiovisual goods and services, "addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market." *Regulation* (EU) 2018/302 (approved February 28, 2018; in effect on December 3, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0302.

35. European Commission, "Digital Single Market: EU Negotiators Agree on New Rules Allowing Europeans to Travel and Enjoy Online Content Services cross Borders," news release, Europe.eu, February 7, 2017, http://europa.eu/rapid/press-release_IP-17-225_en.htm.

But ongoing EU efforts to promote a "digital single market," though admirable on many levels, threaten to foreclose content owners' ability to engage in pricing diversity, tailor content packages on a country-by-country basis, and effectively enforce intellectual property laws. Although parity across EU member states with respect to taxation and regulation is generally a laudable objective, mandating that all copyright owners that distribute audiovisual works—including U.S. companies from movie studios to Internet video platforms—treat all EU subjects in an identical manner may well cause some EU residents to pay *more* for online content than they would otherwise. Such a requirement might also undermine the incentive of U.S. firms to invest in creating original programming, especially content aimed at suiting the tastes of European audiences.

Moreover, given the wide variance among EU member states in terms of purchasing power, as well as in preferences, language, and culture, many content owners and distributors currently tailor their streaming video offerings based on the unique characteristics of audiences in each EU member state.[36] Despite the long-term trend of economic convergence within the European Union, among the EU's 28 member states, GDP per capita in 2017 (adjusted for purchasing power parity) ranged from $21,686 in Bulgaria to $106,373 in Luxembourg, with an EU average of $40,890.[37]

If the European Union's goal of achieving a digital single market ends up prohibiting content owners from offering customized packages of streaming video programming to residents of the EU's diverse member states, many of these consumers will likely suffer.

In addition, given the high fixed costs and trivial marginal costs of distributing video content over the Internet, American consumers who enjoy films and shows that Europeans also consume will suffer indirectly, as U.S. content companies will invest less in producing creative works due to the lower potential total revenue.

The United States should lead the way in affirming the freedom of creators and distributors to experiment with creative arrangements for streaming video over the Internet without prescriptive licensing terms dictated by centralized regulatory bodies.

EU Antitrust Law

The European Union, like the United States, enforces a set of laws designed to prevent companies from engaging in anticompetitive conduct that harms consumers.[38] But the EU's recent history of antitrust enforcement suggests a bias against leading American technology companies.

On several recent occasions, the European Commission, which enforces EU antitrust law, has taken extremely punitive actions against U.S. technology firms based on questionable theories of competitive harm. For instance, in 2009, the European Commission levied a $1.26 billion fine

36. *See, e.g.*, Ashley Rodriguez, "This Is the Cheapest Place in the World to Get Netflix," Quartz (June 3, 2017), https://qz.com/996248/this-is-the-cheapest-place-in-the-world-to-get-netflix/.

37. International Monetary Fund, World Economic Outlook Database: WEO Data by Countries, April 2018 Edition, http://www.imf.org/external/pubs/ft/weo/2018/01/weodata/index.aspx.

38. *Compare* 15 U.S.C. §§ 1–38 to Consolidated Version of the Treaty on the Functioning of the European Union arts. 101–109.

against Intel, the leading U.S. semiconductor chip maker, for allegedly disadvantaging its rival AMD.[39] In 2013, the European Commission levied a $732 million fine against Microsoft for allegedly failing to abide by a four-year-old settlement regarding the promotion of browsers other than Microsoft's Internet Explorer to users of the company's Windows operating system.[40] And in 2017, the European Commission levied a $2.7 billion fine against Google for allegedly disadvantaging rivals in its shopping comparison service's search results.[41]

Although EU regulators maintain that these antitrust enforcement actions arose not out of bias against U.S. firms but because of meritorious complaints of anticompetitive conduct, there is ample cause to be skeptical of this claim. This month, the Initiative on Global Markets at the University of Chicago Booth School of Business polled a panel of leading academic economists with a diverse set of ideological perspectives on the question of whether the EU "often uses its antitrust powers to protect EU-based firms from international competition, rather than to promote greater competition in European markets."[42] Although a plurality of the economists surveyed were uncertain about the question, when weighted for confidence, 32 percent of the economists agreed or strongly agreed with the statement—compared to 25 percent who disagreed or strongly disagreed with it.[43]

Several economists have criticized the EU's approach to dominant technology firms, which tends to target companies that succeed in gaining and maintaining a considerable share of a particular market through innovation and progress. Some commentators have attributed this tendency to the EU's historical desire to combat concentrated economic power regardless of its form—without regard to whether a firm that allegedly gains "too much" concentration faces a meaningful threat of disruptive entry from newcomers or fails to serve its consumers more effectively than its rivals.[44]

Perhaps not coincidentally, high-tech innovation in the European Union lags behind the comparatively dynamic information technology sectors in the United States, Asia, and many parts of the developing world. According to the Digital Evolution Index published by the Tufts University Fletcher School in late 2015, "fifteen European countries have been losing momentum since 2008 in

---

39. David Meyer, "Intel Scores Victory (for Now) in Fight Against $1.3 Billion Fine," *Fortune*, September 6, 2017, http://fortune.com/2017/09/06/intel-eu-antitrust-fine-cjeu/. Intel has challenged this fine, which remains subject to pending litigation before the EU's General Court. *Id.*

40. James Kanter, "European Regulators Fine Microsoft, Then Promise to Do Better," *New York Times*, March 6, 2013, https://www.nytimes.com/013/03/07/technology/eu-fines-microsoft-over-browser.html.

41. Daniel Boffey, "Google Appeals against EU's €2.4bn Fine over Search Engine Results," *The Guardian*, September 11, 2017, https://www.theguardian.com/technology/2017/sep/11/google-appeals-eu-fine-search-engine-results-shopping-service. Google has appealed the fine. *Id.*

42. IGM Forum, *Antitrust and International Competition*, June 13, 2018, http://www.igmchicago.org/surveys/antitrust-and-international-competition-2.

43. *Id.*

44. *See, e.g.*, Simon Tilford, *Is EU Competition Policy an Obstacle to Innovation and Growth?* Center for European Reform, 2008, https://www.cer.eu/sites/default/files/publications/attachments/pdf/2011/essay_competition_st_20nov08-1359.pdf.

terms of their state of digital evolution."[45] The United States, by contrast, belongs to the "stand out" category of nations considered by the index.[46]

Antitrust enforcement poses plenty of challenges of its own without governmental bodies employing it as a means of achieving competitive parity with other countries' technology sectors. U.S. leadership in competition law is increasingly important, especially as developing countries work to craft and implement their antitrust regimes.

Thank you for the opportunity to testify before the Committee, and I welcome your questions.

45. Bhaskar Chakravorti, *Is Europe In A Digital Recession?* Fletcher School at Tufts University, October 28, 2015, https://www.weforum.org/agenda/2015/10/is-europe-in-a-digital-recession/.

46. *Id.*

Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Rachel F. Fefer
Analyst in International Trade and Finance

Before

Joint Economic Committee
U.S. Joint Committee

Hearing on

"The Need for U.S. Leadership on Digital Trade"

June 21, 2018

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

CRS TESTIMONY
Prepared for Congress

Search Terms

Trade barriers

Digital trade

Cross border data flows

Localization

International trade

General Data Protection Regulation

GDPR

Chairman Paulsen, Ranking Member Heinrich, and Members of the Joint Economic Committee, thank you for the opportunity to appear before you today on behalf of the Congressional Research Service to discuss "The Need for U.S. Leadership on Digital Trade." My name is Rachel Fefer and I am an Analyst in International Trade at the Congressional Research Service. As requested, my testimony focuses on the possible implications of the increase in digital trade barriers across the globe and how other countries are attempting to set new international standards and rules that may impact market access for U.S. companies and U.S. consumers.

What is Digital Trade?

The internet-driven digital revolution is causing fundamental change to the U.S. and global economy, leading to new modes of communication and information-sharing, business models, sources of job growth and changes to the composition of jobs, and to new policy challenges. Digital technology enables the creation of new goods and services, including, for example, e-books, online education, and online banking services. Digital technology may also affect the production process for traditional goods and services, raising productivity and/or lowering the costs and barriers related to trade flows, such as for supply chain tracking, 3-D printing, or devices or objects connected via the Internet of Things. Digital platforms serve as intermediaries for multiple forms of digital trade, including e-commerce (e.g., eBay), social media (e.g., Facebook), and cloud computing (e.g., Amazon web services). In these ways, digitization pervades every industry sector, creating challenges and opportunities for established and new players.

The increase in digital trade parallels the growth in internet usage globally. Cross-border data and communication flows are part of digital trade; they also facilitate trade and the flow of goods, services, people, and finance, which together are the drivers of globalization and interconnectedness. One estimate shows that although cross-border bandwidth increased 45-fold from 2005 through 2015, it may still grow nine times larger by 2021.[1]

While there is no globally accepted definition of digital trade, the U.S. International Trade Commission (USITC) broadly defines digital trade as follows:

> The delivery of products and services over the Internet by firms in any industry sector, and of associated products such as smartphones and Internet-connected sensors. While it includes provision of e-commerce platforms and related services, it excludes the value of sales of physical goods ordered online, as well as physical goods that have a digital counterpart (such as books, movies, music, and software sold on CDs or DVDs).[2]

The Importance of Digital Trade to the U.S. and Global Economy

In 2016, the digital economy supported 5.9 million U.S. jobs, or 3.9 percent of total U.S. employment, and accounted for 6.5% of current dollar Gross Domestic Product (GDP).[3] Workers in the digital economy earned average annual compensation of $114,275 compared to the economy-wide average of

[1] Jacques Bughin and Susan Lund, "The ascendancy of international data flows," VOX, January 9, 2017.

[2] U.S. International Trade Commission, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, August 2017, p.33, https://www.usitc.gov/publications/332/pub4716.pdf.

[3] Digital economy here is defined primarily in terms of the Internet and related information and communications technologies (ICT), including (1) the digital-enabling infrastructure needed for a computer network to exist and operate, (2) the digital transactions that take place using that system ("e-commerce"), and (3) the content that digital economy users create and access ("digital media"). Source: Kevin Barefoot, Dave Curtis, William Jolliff, Jessica R. Nicholson, Robert Omohundro, *Defining and Measuring the Digital Economy*, U.S. Bureau of Economic Analysis (BEA), March 15, 2018.

$66,498.[4] Four U.S. firms (Amazon, Microsoft, Google, and IBM) were the top global providers of cloud services in 2016.[5]

The USITC estimated global e-commerce to be worth $28 trillion in 2016, of which 86 percent was business-to business activity.[6] Global e-commerce grew by an estimated 44 percent over the past five years. Information and communication technology (ICT) services, a relative U.S. competitive strength, are outpacing the growth of international trade in ICT goods. The United States is the fourth-largest Organization for Economic Co-operation and Development (OECD) exporter of ICT services.[7] ICT-enabled services are those services with outputs delivered remotely over ICT networks, such as online banking or education, and can augment the productivity and competitiveness of goods and other services. In 2016, exports of ICT services totaled $66 billion of U.S. exports while services exports that could be potentially ICT-enabled were another $404 billion, demonstrating the impact of the internet and digital revolution.[8] As digitization is integrated into the broader economy, digital trade could increasingly become the underlying facilitator of many aspects of traditional international commerce.

Digital Trade Barriers

As noted in your committee's *2018 Economic Report of the President*, "Digital trade has been growing rapidly in recent years," but "challenges to the smooth international flow of goods and funds may prevent trade from reaching its most efficient level."[9]

The increase in digital trade raises new challenges in U.S. trade policy, including how best to address new and emerging trade barriers. Protectionist policies can create barriers to digital trade, or damage trust in the underlying digital economy. This could result in fragmenting the internet, lessening any potential gains by limiting organizations' or individuals' access to markets or data. Governments must often attempt to balance a number of legitimate policy objectives related to digital trade including ensuring national security, promoting innovation and competition, and guaranteeing citizens privacy. However, legitimate policy objectives may also be cited as a rationale for actions that are actually intended to protect the domestic market from international competition. The OECD points out three potentially conflicting policy goals in the internet economy: (1) enabling the internet through regulation without hindering innovation; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers more generally.[10]

The U.S. policy, as stated in President Trump's National Security Strategy, is to "advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services" and "promote the free flow of data."[11] Foreign digital trade barriers are specifically recognized in the U.S. Trade Representative (USTR)'s annual National Trade Estimate Report.[12] The report identifies a number

[4] Ibid.

[5] U.S. International Trade Commission, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, August 2017, p.33, https://www.usitc.gov/publications/332/pub4716.pdf.

[6] Ibid.

[7] In 2016, the largest exporters of ICT services were Ireland, India, and the Netherlands. OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-en.

[8] Bureau of Economic Analysis (BEA), https://bea.gov/scb/pdf/2017/10-October/1017-international-services-tables.pdf.

[9] U.S. Congress, Joint Economic Committee, *The 2018 Joint Economic Report*, committee print, 115th Cong., 2nd sess., March 13, 2018, 115-596, p. 48.

[10] Koske, I. et al. (2014), "The Internet Economy - Regulatory Challenges and Practices," OECD Economics Department Working Papers, No. 1171, OECD Publishing, Paris. DOI, http://dx.doi.org/10.1787/5jxszm7x2qmr-en.

[11] The President of the United States, "National Security Strategy of the United States of America," December 2017.

[12] https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

of individual country policies across the globe that may impact U.S. digital trade, illustrating the breadth and variety of digital trade barriers (see **Figure 1**). Digital trade barriers, many of which are highlighted in the report, include:

- **High tariffs**. Tariffs on ICT or digital goods or services may raise costs for sellers and potentially result in higher prices for buyers. Though World Trade Organization (WTO) agreements and U.S. free trade agreements (FTAs) eliminate tariffs on most ICT goods and digital trade, some countries have considered tariffs to raise revenue and protect domestic industries.[13] Exemption from duties and simplified customs procedures for low-value shipments (i.e., a *de minimus* threshold) can facilitate trade and expand e-commerce exports. Raising *de minimus* levels may be especially important for U.S.-based small and mid-sized enterprises (SMEs) seeking to export, because the United States has a relatively high *de minimus* threshold ($800) compared to many U.S. trading partners (Canada's *de minimus*, for example, is C$20, approximately $15, recently).
- **Localization requirements**. Governments may use privacy or national security arguments as justifications to compel companies to conduct certain digital-trade-related activities within a country's borders such as manufacturing or data processing.
- **Cross-border data flow limitations**. Regulations limiting cross-border data flows and requiring local storage are a type of localization requirement that prohibits companies from exporting data outside a country. Governments may claim legitimate policy objectives such as protecting privacy or cybersecurity as justifications for data localization measures. These restrictions can pose barriers to companies whose transactions rely on the internet to serve customers abroad, manage global value chains, and operate more efficiently. Limiting the ability to move data across national lines may constrain the ability to use innovative technologies such as blockchain applications because cross-border data flows are needed to share and store data on a blockchain with global partners for supply chain tracking, trade finance, customs and border clearance, or other international transactions.

  According to a 2017 USITC report, U.S. firms cited data localization as the top policy measure impeding digital trade, and the number of data localization measures globally has doubled in the last six years.[14] One U.S. business group noted increased forced localization measures, citing examples in China, Colombia, the European Union (EU), Indonesia, South Korea, Russia, and Vietnam,[15] while another highlighted barriers to cloud services in Indonesia, Russia, and Vietnam.[16]
- **Intellectual property rights (IPR) infringement.** IPR infringement includes copyright piracy, counterfeiting of trademarks, circumvention of technological protection measures (TPMs), cyber-theft of trade secrets, and trademark infringement related to domain names. By its nature, IPR infringement is difficult to quantify, and doing so in the digital environment is all the more challenging given that, for example, "infringing files are traded online and websites offering counterfeits are launched and accessed, countless

[13] During the 2017 WTO Ministerial meeting, some African countries suggested discontinuing the current moratorium. Communication from the African Group, *Draft Ministerial Decision on Electronic Commerce*, November 20, 2017.

[14] USITC, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, https://www.usitc.gov/publications/332/pub4716.pdf.

[15] Information Technology Industry Council, Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses, August 1, 2017, http://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf.

[16] Business Software Alliance, 2018 BSA Global Cloud Computing Scorecard, http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf.

times each day."[17] According to USTR, online sales of pirated and counterfeit goods reportedly could exceed the volume of sales "through traditional channels such as street vendors and other physical markets." A 2016 International Chamber of Commerce (ICC) study estimated the value of digitally pirated music, movies, and software (not actual losses) as $213 billion in 2013 to potentially $384-$856 billion in 2022.[18]

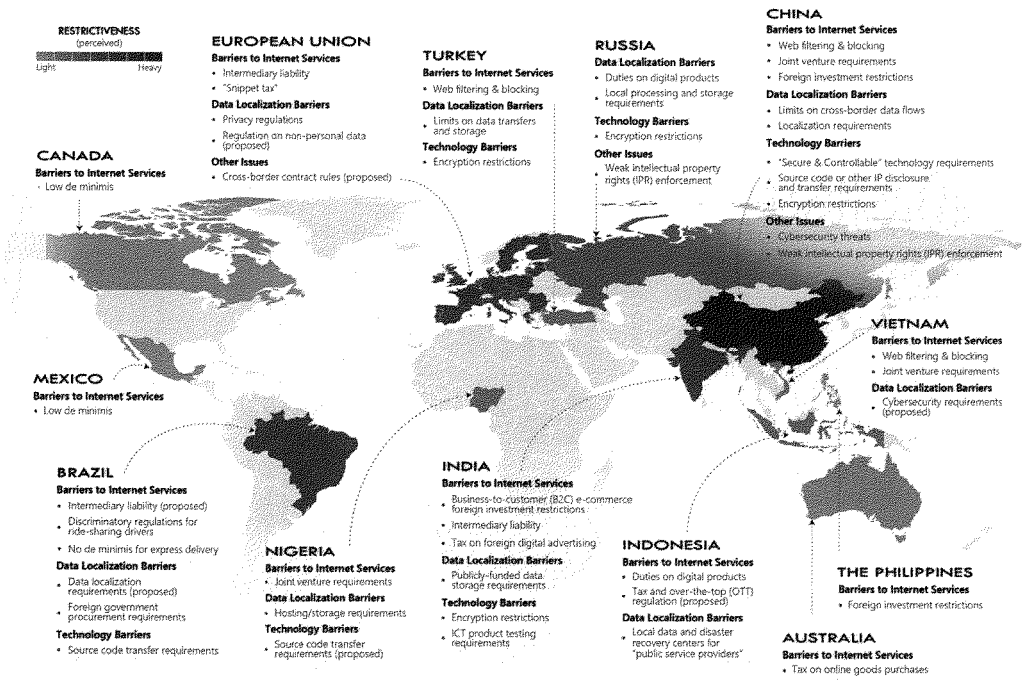
- **Discriminatory, unique standards or burdensome testing**. Local or national standards that deviate significantly from recognized international standards may limit interoperability or increase costs, and redundant testing or local registration requirements may make it difficult to enter or deter firms from entering a particular market.
- **Filtering or blocking of online content**. Governments may seek strict control over digital data within their borders, such as what information people can access online, and how information is shared inside and outside its borders.
- **Restrictions on electronic payment systems**. Lack of access to online payment options by foreign providers restricts the ability for companies or customers to sell and purchase online.
- **Cybersecurity concerns** including:
  - **Cyber-theft of U.S. trade secrets**. Cyber-attacks in general are deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. According to the White House Council of Economic Advisers, malicious cyberactivity (i.e., business disruption, theft of proprietary information) cost the U.S. economy up to $109 billion in 2016.[19]
  - **Forced technology transfer or restrictive cyber-security laws**. Requiring a firm to transfer its proprietary technology or reveal its source code in order to gain market access may deter firms from entering a market or undermine their competitiveness.
  - **Restrictions on cryptography and the use of encryption**. Limiting the ability to encrypt data, or controlling the type of encryption used, may expose a company to cybersecurity risks, serving as a deterrent to market entry.

[17] ITC, Digital Trade in the U.S. and Global Economies, Part 1, USITC Publication 4415, July 2013, p. 5-15.

[18] USTR, 2017 Special 301 Report, April 2017; Frontier Economics, The Economic Impacts of Counterfeiting and Piracy, report commissioned by Business Action to Stop Counterfeiting and Piracy (BASCAP) of the International Chamber of Commerce (ICC), June 2017.

[19] Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy, February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Figure 1. Levels of Perceived Digital Trade Barriers in Selected Countries



Source: CRS analysis based on U.S. Trade Representative, 2018 National Trade Estimate Report on Foreign Trade Barriers, available at https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

Notes: *This map may be used in other CRS products. This map is illustrative of prominent digital trade barriers and not meant to be an exhaustive list

Digital Trade Rules

No single set of international rules or disciplines governs digital trade issues. Given the stalemate in the WTO negotiations, multilateral trade agreements have not kept pace with the complexities of the digital economy and digital trade is treated unevenly in existing WTO agreements. The rules are evolving piecemeal as governments experiment with different approaches and consider diverse policy priorities and objectives. These diverse country-specific rules may not always align with U.S. goals or policies.

Policies that affect digitization in any one country's economy can have consequences beyond its borders, and because the internet is a global "network of networks," the state of a country's digital economy can have global ramifications. The lack of globally accepted rules and standards for digital trade means that individual economies around the world are creating their own rules and regulations impacting market access. For my testimony, I will focus on two large economies and how they are shaping international rules. China and the EU each use their market size to set terms that other trading partners, and U.S. companies seeking to do business in their markets, must follow.

China

With a fundamentally distinct approach to the Internet compared to Western countries, China presents a number of significant opportunities and challenges for the United States in digital trade. In 2008, China overtook the United States as the world's largest Internet user (at 299 million versus 225 million users).[20] As of April 2017, China had 717.3 million Internet users.[21] China is the world's largest market for retail E-commerce, making it an attractive market for U.S. businesses. In 2016, China's E-commerce sales were estimated at $911 billion compared to $384 billion for the United States. [22] However, China's policies and actions have limited the ability of U.S. firms to enter or compete in the Chinese market.

Internet Sovereignty

The Chinese government has sought to advance its views on how the Internet should be expanded to promote trade, but also to set guidelines and standards over the rights of governments to regulate and control the Internet, a concept it has termed "Internet Sovereignty."[23] The Chinese government appears to have first advanced a policy of "Internet Sovereignty" around June 2010, stating:

> "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security."[24]

[20] *Internet World Stats*, 2017, available at http://www.Internetworldstats.com/stats3.htm.

[21] Newzoo, *Top 50 Countries by Smartphone Users and Penetration*, 2017, available at https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.

[22] eMarketer, *Worldwide retail eCommerce Sales: iMarketer's Updated Estimates and Forecast Through 2019*, 2016, available at https://www.emarketer.com/public_media/docs/eMarketer_eTailWest2016_Worldwide_ECommerce_Report.pdf.

[23] Originally, China appeared to be mainly focused on establishing Internet rules domestically, but over the past few years it appears to be advancing its vision of Internet sovereignty globally.

[24] The People's Daily, *Full Text: The Internet in China*, June 8, 2010, available at http://en.people.cn/90001/90776/90785/7017202.html.

In December 2016, the Chinese government issued a National Cybersecurity Strategy, that emphasized China's view of cyber sovereignty and its right to promulgate policies in line with its own priorities without other countries interfering in its cyberspace.[25]

China has erected what is termed by some as the "Great Firewall," censoring and limiting what websites and information is available through the Internet in China. A 2018 report by the USTR cited a number of Internet-related barriers, noting that China currently blocks 12 of the top 30 global sites and up to 3,000 sites in total, limiting U.S. companies' access to Chinese customers.[26] A change to China's internet filters also blocks virtual private network (or VPN) access to sites beyond the Great Firewall. VPNs have been used by individuals and businesses in China to access websites like Facebook or data (e.g., information from foreign subsidiaries or partners) outside of China.[27]

China's Internet sovereignty initiative represents its assertion that the government has the right to limit information and fully control the Internet within China while some see it as further evidence of a more assertive Chinese foreign policy. Other critics of China's Internet Sovereignty policy view it as an attempt by the government to limit market access by foreign Internet, digital, and high technology firms in China, in order to boost Chinese firms and reduce China's dependence on foreign technology.

Cybersecurity Law

On November 7, 2016, the Chinese government passed a new Cybersecurity Law, that came into effect June 1, 2017. The American Chamber of Commerce in China (AmCham China) noted in particular the law's broad restrictions on cross-border data flows, and warned that they would "create barriers to Chinese as well as foreign companies operating in industries where data needs to be shared internationally."[28] The law's data localization requirements create a barrier to companies that want to use U.S. cloud-based services to access or better serve Chinese customers, share information with headquarters or subsidiaries abroad, or use innovative technologies such as blockchain[29] that depend on free flow of information.

A 2017 USTR report cited "significant declines in commercial sales of foreign ICT products and services in China," as evidence that China continued to maintain "mercantilist policies under the guise of cybersecurity."[30] Some analysts have expressed concerns that one of the main goals of the new cybersecurity law is to promote the development of indigenous technologies and impose restrictions on foreign firms. For example, the law states that "critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, and be safety certified by a qualified establishment or meet the requirements of a safety inspection, before being sold or provided."[31] The new law mandates reviews by the Cyberspace Administration of China (CAC) on foreign and domestic technology suppliers to ensure that their technology is "secure and controllable."

---

[25] China Copyright and Media, National Cyberspace Security Strategy, December 27, 2016, available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

[26] USTR, *2018 National Trade Estimate Report on Foreign Trade Barriers*, March 2018.

[27] Yu Nakamura, "China's war on VPNs creates havoc at foreign companies," December 17, 2017.

[28] AmCham China, *AmCham China Statement on Cybersecurity Law*, November 7, 2017, at https://www.amchamchina.org/about/press-center/amcham-statement/amcham-china-statement-on-cybersecurity-law.

[29] Blockchain is a distributed record-keeping system (each user can keep a copy of the records) that provides for auditable transactions and secures those transactions with encryption. Using blockchain, each transaction is traceable to a user, each set of transactions is verifiable, and the data in the blockchain cannot be edited without each user's knowledge.

[30] USTR, *2017 Report to Congress on China's WTO Compliance*, January 2018, p. 3.

[31] See translation of the law at http://chinalawtranslate.com/cybersecuritylaw/?lang=en#LBQMwbmaWhGozeMj.99.

The CAC can also refuse to certify a product for unspecified risks to national security.[32] The term "secure and controllable" is another ambiguous term that has not been fully defined by Chinese authorities, raising concerns that it could be used as a process either to lock out foreign technology firms in China or force them to transfer technology and share proprietary information, such as source code (to demonstrate that there are no vulnerabilities that hackers can exploit), with Chinese regulators or partners.

IPR Theft

China is considered by most analysts to be the largest source of global theft of IP and a major source of cyber theft of U.S. trade secrets, including by government entities, deterring some U.S. firms from entering the Chinese market and potentially limiting the profitability of those that do. American firms cite the lack of effective and consistent protection and enforcement in China of U.S. IPR as one of the largest challenges they face in doing business in China.[33] Although China has improved its IPR protection regime over the past few years, many U.S. industry officials view piracy rates in China as unacceptably high. A 2017 survey by the U.S.-China Business Council found that 94% of respondents said they were concerned about IPR in China.[34]

Technology transfer requirements, whether formal through regulations limiting foreign investment or requiring joint ventures, or informal by applying pressure on companies seeking to do business in China, are a major complaint of U.S. firms seeking to protect their proprietary information. A 2018 USTR Section 301 investigation into Chinese laws, policies, practices, and actions that may harm American IPR, innovation, or technology development concluded that China (1) uses joint venture requirements, foreign investment restrictions, and administrative review and licensing processes to force or pressure technology transfers from American companies; (2) uses discriminatory licensing processes to transfer technologies from U.S. companies to Chinese companies; (3) directs and facilitates investments and acquisitions that generate large-scale technology transfer; and (4) conducts and supports cyber intrusions into U.S. computer networks to gain access to valuable business information. The USTR estimated that such policies cost the U.S. economy at least $50 billion annually.[35]

China's Influence on Other Countries

China's FTAs have limited commitments on digital trade. For example, the Australia-China FTA contains a chapter on electronic commerce, with provisions relating to the prohibition of customs duties on electronic transmissions, regulatory transparency, and consumer protection among others. However, it is not enforceable through the agreement's dispute settlement procedures, potentially limiting its effectiveness.

Many analysts argue that China's policies are setting protectionist precedents globally, limiting market access to U.S. or other foreign firms and potentially splintering or fragmenting the Internet. Other countries have sought to imitate China's policies by requiring local data storage and limiting cross-border data flows, filtering and censoring online content, or requiring access to source code in the name of

[32] Eva Dou, "China to Start Security Checks on Technology Companies in June," *Wall Street Journal*, May 3, 2017, https://www.wsj.com/articles/china-to-start-security-checks-on-technology-companies-in-june-1493799352.

[33] U.S.-China Business Council, *2017 Member Survey*, p. 10, available at https://www.uschina.org/sites/default/files/2017_uscbc_member_survey.pdf.

[34] Ibid.

[35] The USTR investigation followed a presidential memorandum and was conducted under Section 301 of the Trade Act of 1974. For more information on the Section 301 investigation, see CRS In Focus IF10708, *Enforcing U.S. Trade Laws: Section 301 and China*, by Wayne M. Morrison.

national security or cybersecurity. As noted above, Russia and Vietnam have used cybersecurity as a rationale for laws that require local data storage.

European Union

While the United States and the EU share broad objectives for an open and rules-based international trading system, particular differences in policies may have ramifications on digital flows and international trade with significant economic consequences given the size of the trading relationship. The transatlantic economy accounts for half of the global gross domestic product by value,[36] and cross-border data flows between the United States and EU are the highest in the world. As of 2016, the United States and EU traded $2.7 billion a day worth of goods and services, and the annual digital services trade between the two regions is approximately $260 billion.[37] The two partners' varying approaches to digital trade, privacy, and national security, have, at times, threatened to disrupt U.S.-EU data flows.

Data Privacy and Protection

The United States and EU have different legal approaches to information privacy that extends into the digital world. The EU considers the privacy of communications and the protection of personal data to be fundamental rights, which are codified in EU law. Europe's history with fascist and communist regimes informs the EU's views on data protection and contributes to the demand for strict data privacy controls. The EU regards U.S. data protection safeguards as inadequate; this has complicated the conclusion of U.S.-EU information-sharing agreements and raised concerns about U.S.-EU data flows that many U.S. firms depend on to access EU customers and operate efficiently.

After extensive negotiations, the EU-U.S. Privacy Shield became operational in August 2016, providing a framework to provide U.S. and EU companies a mechanism to comply with data protection requirements when transferring personal data between the EU and the United States.[38] Under the Privacy Shield program, U.S. companies can voluntarily self-certify compliance with requirements such as robust data processing obligations. The agreement includes obligations on the U.S. government to proactively monitor and enforce compliance by U.S. firms, establish an ombudsman in the U.S. State Department, and set specific safeguards and limitations on surveillance. The Privacy Shield also involves an annual joint review by the United States and the EU, the first of which was conducted in September 2017.[39] The United States and Switzerland also agreed to the Swiss-U.S. Privacy Shield, which will be "comparable" to the U.S.-EU agreement.[40]

Subsequent to the signing of Privacy Shield, the EU agreed on a new General Data Protection Regulation (GDPR), which became applicable on May 25, 2018. The GDPR established a single set of rules for protection of personal data throughout the EU that seeks both to strengthen individual fundamental rights in the digital age and facilitate business by ensuring more consistent implementation of the rules EU-

[36] http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/.

[37] Penny Pritzker, Former U.S. Secretary of Commerce and Andrus Ansip, Vice-President of the European Commission for the Digital Single Market, "Making a Difference to the World's Digital Economy: The Transatlantic Partnership," March 11, 2016, https://www.commerce.gov/news/blog/2016/03/making-difference-worlds-digital-economy-transatlantic-partnership.

[38] For more information on the Privacy Shield, see CRS Report R44257, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, by Martin A. Weiss and Kristin Archickand https://www.privacyshield.gov/Program-Overview.

[39] Department of Commerce, U.S. Secretary of Commerce Wilbur Ross Welcomes Release of the European Commission's Report on the EU-U.S. Privacy Shield, October 18, 2017, https://www.commerce.gov/news/press-releases/2017/10/us-secretary-commerce-wilbur-ross-welcomes-release-european-commissions.

[40] Lauren Cerulus, "Switzerland and U.S. strike 'privacy shield' data transfer deal," Politico Pro, January 11, 2017.

wide. The GDPR is seen by some as the most comprehensive privacy regulation impacting digital trade globally and potentially precedent-setting for how businesses conduct themselves in regards to personal data.

The GDPR identifies what is a legitimate basis for data processing and sets common rules regarding data retention, storage limitation, and record keeping. Processing certain sensitive personal data is generally prohibited. Stronger and new data protection requirements grant individuals the right to:

- Receive clear and understandable information about who is processing one's personal data and why;
- Consent affirmatively to any data processing;
- Access any personal data collected;
- Rectify inaccurate personal data;
- Erase one's personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data (the "right to be forgotten");
- Restrict or object to certain processing of one's data;
- Be notified without "undue delay" of a data breach if there is a high risk of harm to the data subject; and
- Require the transmission of one's data to another controller (data portability).

The potential high penalties for non-compliance have attracted significant attention since a company or organization can be fined up to 4% of its annual global turnover or €20 million (whichever is greater). Fines are to be assessed by the national supervisory authority (a Data Protection Authority, or DPA) in each member state and subject to appeal in national courts. Some stakeholders are concerned about possible uneven enforcement by EU Member States. The GDPR also requires some companies to hire data protection officers.[41]

U.S. firms have voiced several concerns about the GDPR, including how it is implemented and the scale of potential fines. Some companies are concerned about the need to construct a compliance bureaucracy and possible high costs for adhering to the GDPR's requirements. While large firms have the resources to hire consultants and lawyers, it may be harder and costlier for SMEs to comply, possibly deterring them from entering the EU market and creating a de facto trade barrier. Reports suggest that some SMEs have opted to exit or limit offerings or services to the EU market given the complexities of complying with the GDPR, possibly limiting competition and customer choice.

Another issue is that the GDPR right to erasure could clash with freedom of information, and, for U.S. firms, with the First Amendment. The GDPR includes exceptions and recognizes the need to balance the right to personal data protection with freedom of expression, but advocates worry that Internet companies may be quick to grant erasure requests to avoid possible legal challenges, which, over time, could erode information online. Many Internet companies share such concerns, viewing the GDPR erasure provisions as pitting the "right to be forgotten" against the "right to know."

Under the GDPR, the U.S.-EU Privacy Shield will continue to serve as a mechanism for participating U.S. and EU companies that meet EU data protection requirements. However, Privacy Shield is not a GDPR compliance mechanism and participation by a company in Privacy Shield does not guarantee full GDPR compliance.

[41] For more information on the GDPR, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick, and https://www.eugdpr.org/.

Some observers and government officials worry about the potential negative impact of the GDPR on innovation, including the use of blockchain or artificial intelligence, and on the WHOIS database (managed by the Internet Corporation for Assigned Names and Numbers, or ICANN) that stores information about the registrants and operators of websites.[42] Law enforcement and cybersecurity researchers often use WHOIS to identify hackers and malicious Internet domains. WHOIS data could now be protected under the GDPR, and some worry this will undercut WHOIS as an effective cybersecurity tool. ICANN has begun filing legal action in EU countries restricting access under GDPR.[43]

In addition to GDPR, the EU's draft ePrivacy Regulation has also raised concerns among companies and industry groups who see the current proposal bringing digital communications under the same rules as traditional telecommunications as too onerous and restrictive.[44] While some advocate the regulation as needed consumer protection to ensure the privacy of electronic communications, others voice concern that it may hinder innovation gains of machine-to-machine communication or Internet of Things (IoT) applications. As GDPR went through multiple drafts being finalized, the ePrivacy Regulation may be further refined as it goes through the EU legislative process.

EU Influence on Other Countries

In its free trade negotiations with other countries, the EU has few hard commitments in regard to digital trade apart from prohibiting customs duties on electronic deliveries; instead it emphasizes regulatory dialogue. Cross-border data flows are not protected under EU FTAs and the EU did not want to include the topic in the U.S.-EU Transatlantic Trade and Investment Partnership (TTIP) negotiations under the Obama Administration. For example, the Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada, the most recent EU FTA that has entered into force, establishes a dialogue on multiple digital trade issues and requires parties to have measures to protect personal information of users but does not explicitly require a GDPR-like regime.[45] CETA does not mention cross-border data flows nor are data flows addressed in the EU-Japan FTA, which has yet to be ratified by the EU, although the parties agree to discuss the issue in the future.[46]

As no multilateral rules on cross-border data flows or data privacy exist, some experts contend that the GDPR may effectively set new global data privacy standards as companies and organizations strive for compliance to avoid being shut out of the EU market. Some companies may determine that it is easier to comply with EU regulations globally rather than implement changes for only the EU market. "In the absence of another approach, it's easier for other markets to follow what Europe has done," said Dean C. Garfield, president of the Information Technology Industry Council.[47]

Regarding privacy, European Commissioner for Justice, Consumers and Gender Equality, Vera Jourova, has stated, "We want to set the global standard."[48] Some countries are adopting GDPR-like regimes to

[42] ICANN, "Data Protection/Privacy Update: Seeking Additional Clarity from Article 29," May 10, 2018.

[43] ICANN, "ICANN Files Legal Action in Germany to Preserve WHOIS Data," May 25, 2018, https://www.icann.org/news/announcement-2018-05-25-en.

[44] For more information on the ePrivacy Regulation, see https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[45] EU-Canada Comprehensive Economic and Trade Agreement (CETA) Chapter 16 Electronic Commerce, http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/.

[46] Proposal for a Council Decision on the conclusion of the Economic Partnership Agreement between the European Union and Japan, Article 8.87, April 18, 2018.

[47] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *New York Times*, May 24, 2018.

[48] Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide," *PolitocPro*, (continued...)

ensure that the EU allows for cross-border data flows between the parties,[49] to facilitate domestic companies doing business in the EU, or as a short-cut to establishing a domestic privacy framework.[50] Countries such as Brazil, Japan, and South Korea have explicitly sought advice from the EU for their own data protection laws while others aim to update their rules to meet EU levels. U.S. privacy advocates have encouraged U.S. firms to adopt changes made to comply with the GDPR in the United States as well, viewing the changes as advancing consumer protection. Privacy and consumer advocates have also voiced support for the establishment of a comprehensive U.S. privacy policy similar to the GDPR.

Establishing International Digital Trade Rules

Some view China and the EU as seeking to impose their views and standards globally, using their large market size to guide international practices. These observers contend that the United States should proactively counter Chinese and EU efforts to move forward with new digital trade policies that may limit market access to U.S. firms. Some analysts suggest that the United States should focus attention on developing new digital trade rules and disciplines through ongoing and future bilateral and plurilateral trade negotiations in line with U.S. policy and priorities.

Trade Promotion Authority

The growth in trade barriers has raised the prominence of digital trade on the trade agenda. Congress recognized the importance of digital trade and removing related barriers in the negotiating objectives of its most recent grant of Trade Promotion Authority (TPA), the Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114-26), signed into law in June 2015.[51] TPA 2015 objectives related to digital trade direct the Administration to negotiate agreements that:

- ensure application of existing WTO commitments to the digital trade environment, ensuring no less favorable treatment to physical trade;
- prohibit forced localization requirements and restrictions to digital trade and data flows;
- keep electronic transmissions duty-free; and
- ensure relevant legitimate regulations are as least trade restrictive as possible.

Negotiating Forums

Some see a risk to U.S. market access and influence if the Unites States does not actively seek to establish new international trade rules while large economies such as China and the EU push forward with policies reflecting their vision of the Internet and digital trade.

The proposed Trans-Pacific Partnership (TPP), negotiated by the United States during the Obama Administration, was seen by some as having the most comprehensive digital trade commitments of any

(...continued)

February 6, 2018.

[49] Countries may seek "adequacy" decisions by the EU to allow for cross-border data flows. The U.S.-EU Privacy Shield serves as an alternative to a full adequacy decision by the EU.

[50] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *New York Times*, May 24, 2018.

[51] For more information on TPA, see CRS In Focus IF10038, Trade Promotion Authority (TPA), by Ian F. Fergusson, and CRS Report RL33743, Trade Promotion Authority (TPA) and the Role of Congress in Trade Policy, by Ian F. Fergusson.

FTA to date. The TPP aimed to promote digital trade, promote the free flow of information, and ensure an open internet.[52] After President Trump withdrew the United States from the TPP, the eleven remaining countries negotiated and signed a revised agreement without the United States, which is now in the ratification process. The revised TPP, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), made modifications to select IPR and investment commitments but largely retained the provisions of the original agreement, including on digital trade.[152] For example, the CPTPP requires parties to have a legal framework to protect personal information. Privacy frameworks such as the EU's GDPR and the international Asia-Pacific Economic Cooperation (APEC) Privacy Framework and Cross Border Privacy Rules (CBPRs) (to which the United States belongs) would be permitted under the CPTPP provisions.[53] Some view the TPP as a lost opportunity for the United States to set global rules and best practices on digital trade.

New and ongoing bilateral and plurilateral negotiations present opportunities for the United States to establish rules and disciplines on digital trade.

- **North American Free Trade Agreement (NAFTA).** Like the Uruguay Round agreements, which created the WTO, NAFTA also entered into force in the 1990's, predating mass usage of the internet. The ongoing NAFTA renegotiations provide an opportunity to address digital trade.[54] Some have suggested the TPP text could provide a starting point while others contend that the revised NAFTA should go beyond those commitments such as by specifying a *de minimus* standard. Canada and Mexico may soon be party to similar commitments through their participation in the CPTPP.
- **E-commerce Plurilateral**. In December 2017, on the sidelines of the 11th WTO Ministerial Conference in Buenos Aires, Argentina, a group of over 70 WTO members, including the United States, agreed to "initiate exploratory work together toward future WTO negotiations on trade related aspects of electronic commerce."[131] USTR supported the movement toward plurilateral efforts stating, "the United States is pleased to work with willing Members on e-commerce, scientific standards for agricultural products, and the challenges of unfair trade practices that distort world markets."[132] Members are currently discussing which aspects of digital trade they will address in any negotiations. The United States put forth its objectives, including market access, data flows, fair treatment of digital products, protection of intellectual property and digital security measures, and intermediary liability, among others.[133]
- The **G-20, OECD**, **APEC**, and bilateral forums all provide international venues outside of trade negotiations that can be used to establish high-level, nonbinding best practices and principles and align expectations on digital trade.
- **Technology Transfer.** In May 2018, the United States, the EU, and Japan agreed to "deepen cooperation and exchange of information, including with other like-minded partners, to find effective means to address trade-distorting policies of third countries, including harmful forced technology transfer policies and practices, and where appropriate, to pursue dispute settlement proceedings at the WTO."[55] The three agreed to establish and share best practices and work together to end technology transfer policies by other countries.

[52] For more information, see CRS In Focus IF10390, *TPP: Digital Trade Provisions*, by Rachel F. Fefer.

[53] For more information on the APEC Privacy Framework, see https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

[54] U.S. Trade Representative, *Summary of Objectives for the NAFTA Renegotiation*, November 2017, https://ustr.gov/sites/default/files/files/Press/Releases/Nov%20Objectives%20Update.pdf.

[55] U.S. Trade Representative Press Release, "Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, Japan, and the European Union," May 2018.

Testimony before the United States Congress Joint Economic Committee

Ambassador Robert W. Holleyman
President & CEO, C&M International & Partner, Crowell & Moring LLP

Hearing on "*The Need for U.S. Leadership on Digital Trade*"
June 23, 2018

Chairman Paulsen, Ranking Member Heinrich, and members of the Committee, thank you for the opportunity to testify on a topic that is of critical importance to the United States' economic future. Digital issues and trade have been central to my work for nearly three decades.

I have three brief points that I'd like to make today and then look forward to our discussion.

THE STAKES ARE HIGH:

First, United States' leadership on digital trade is not simply a priority of "tech" companies, or for executives in regional tech hubs. It is an imperative for all Americans to compete in the 21st-century global economy. It is important to traditional manufacturers; to small businesses integrated into global supply chains; to farmers using weather and planting data; entrepreneurs developing the next revolutionary technology; and to small, "mom-and-pop" operations looking to take advantage of the global e-commerce opportunities and new markets enabled by the Internet. All of us now live in a world shaped by the immense opportunities provided by a global, digital economy.

I share the view of your Vice Chairman, Senator Lee, from this Committee's hearing last fall on the gains from free digital trade for the U.S. economy. He stated that "we are swiftly approaching the point at which the word 'digital' will be an unnecessary adjective for trade." I couldn't agree more. So-called "digital" issues underpin all aspects of our economy. They drive the fastest-growing, most competitive sectors of the U.S. economy.

I just returned this past weekend from travel in Hong Kong and Beijing. And I can tell you, first-hand, that innovative companies abroad – competitors to U.S. firms and American workers – are acting swiftly to gain a next-generation advantage in the digital space, in areas ranging from mobile payments to cloud computing to content delivery. They are capturing an increasing market share in the world's fastest growing economies.

And as the digital economy is evolving at an exponentially rapid pace, so, too, is the global policy and regulatory landscape. Foreign governments – both allies and adversaries – are actively establishing their leadership by charting new regulatory regimes and rules that will help define who wins and who is left behind in the digital economy. In many cases, they are erecting barriers that – if left unchecked – may significantly harm the ability of companies based in the U.S. to access global markets and customers.

Breaking down barriers to digital trade is essential to opening markets for America's most innovative, thriving industries, and is foundational to the future competitiveness of the United

States, our economy and workers. This was central to my work as Deputy United States Trade Representative. To assess digital trade and quantify the impact of digital trade barriers, in January of 2017, following recommendations from USTR's Digital Trade Working Group, which I chaired, Ambassador Mike Froman directed the United States International Trade Commission to undertake a three-part study on the global outlook for digital trade.

The ITC delivered its first report in August of last year. While it outlined the substantial economic impact and business opportunities provided by digital trade, it also catalogued numerous policy trends that are inhibiting American competitiveness in the field. These include common trade challenges like market access barriers, investment limitations, and lax protection for intellectual property. The ITC also reported on a series of unique challenges to digital trade: new, protectionist walls being erected to carve up the global marketplace and provide advantages to local, favored players. The ITC identified problems related to foreign provisions on data protection and data localization, cybersecurity, trade-distorting privacy measures, and source code disclosure requirements.

LEVERAGE OUR TRADE POLICY & NEGOTIATIONS

This leads to my second point: the United States must use our trade might to break down these emerging barriers that inhibit U.S. firms from competing on a level playing field. I commend Ambassador Lighthizer and the Office of the United States Trade Representative for continuing to shine a light on restrictive, protectionist barriers to digital trade erected by other countries, in its annual National Trade Estimate report. We started this practice in the Obama Administration to call attention to and put laser-like focus on digital barriers, recognizing that the U.S. needed to act quickly to identify and combat barriers to digital trade before they become enshrined. We also appreciated the strong bipartisan Congressional interest in digital trade, as this hearing and its predecessor shows.

Unfortunately, the broader approach that this Administration has taken on trade is not only causing deep uncertainty within the American business community, it is crowding out the attention that could be focused on digital trade and our economic future. We need allies like Canada, Mexico and Japan to join us in establishing the rules of the road for the digital economy. We need our allies in fighting against the rise of digital barriers. It is hard to set the course for our future economy when we are fighting over new tariff taxes.

The U.S. must demonstrate leadership by flexing the muscle of American trade policy on issues related to digital trade in all our negotiations with trade partners. The digital trade-related provisions negotiated in the Trans-Pacific Partnership created a new paradigm for a 21st-century trade agreement that creates a level, fair, competitive landscape for the digital economy. Eleven of our would-be trading partners from the TPP – ranging from Japan and Australia, to Mexico and Singapore – continue to advance high-standard digital trade through their adoption of the new Comprehensive and Progressive Agreement for Trans-Pacific Partnership, or CPTPP.

The TPP, and now CPTPP, contain a series of provisions we dubbed "the Digital Two Dozen" – which can serve as a template for our future trade negotiations. USTR has advanced substantially similar provisions in the NAFTA negotiations with Canada and Mexico. We must continue to do so and secure this new model for the future of digital trade in North America and beyond.

While the Administration looks to country-specific trade negotiations, we also know that the digital economy and barriers to digital trade are growing faster than any one or series of bilateral trade negotiations can address. To truly shift the paradigm and assert American leadership on digital trade, therefore, we must look beyond bilateral negotiations. We must be bold and expansive in our thinking. It is time for a new, plurilateral initiative, bringing together likeminded allies and partners, and focused on setting a harmonized, market-oriented framework for digital trade. Such a new initiative could be modeled on our successful efforts to negotiate and then expand the Information Technology Agreement. U.S. leadership in this area helped reduce barriers and costs and expand the markets for IT products and services globally – to the benefit of U.S. companies. A new digital trade negotiation, championed by the United States, and likely in concert with our NAFTA and TPP trading partners, could ensure that our nation leads in setting the rules for the digital economy and digital trade as we have done before in the ITA.

LEADERSHIP ON DATA FLOWS, DATA PROTECTION, & PRIVACY

Finally, the United States must take a firm stance to ensure that the free flow of data, which is foundational to the digital economy, is regulated in a measured, smart way. As the ITC noted in its report, "fully half of all global trade in services now depend[s] on access to cross-border data flows." And among all the emerging policy issues that caused concern, the most-cited measure impeding digital trade was forced data localization.

If "data is the new oil," fueling the growth of digitally-intensive industries and trade, then we have to regulate the movement of this 21st-century fuel with a balanced, thoughtful approach. One that respects personal privacy protections and security, first and foremost; but one that also ensures that protected and general data can cross borders, since the digital economy is truly global, integrated, and, in some respects, borderless.

Right now, however, it is widely acknowledged that the European Union is setting the rules of the road for data privacy, with last month's implementation of the EU General Data Protection Regulation (GDPR). Let's be clear: the GDPR is a European model, focused on the protection of European citizens. It's also a model that the EU would like to see exported to markets all around the world.

While the GDPR has advanced the discussion around privacy, we know that privacy protection is not simply of interest to European citizens. We know that privacy matters to Americans and others globally; we know, too, that it can be advanced and respected as a foundational part of the global digital economy. With that in mind, the United States helped launch the APEC Cross-Border Privacy Rules alongside twenty other nations within the Asia-Pacific Economic Cooperation forum, or APEC, nearly a decade ago. The CBPRs were created to ensure the protection of personal, private information; but, in a balanced way that is also pro-growth, pro-innovation, and ensures that we can all harness the opportunities and benefits of the digital economy. As the ITC report notes, U.S. companies favor the APEC approach because it "sets a high standard of privacy across member countries without 'interrupting or threatening the flow of data that fuel economic growth.'"

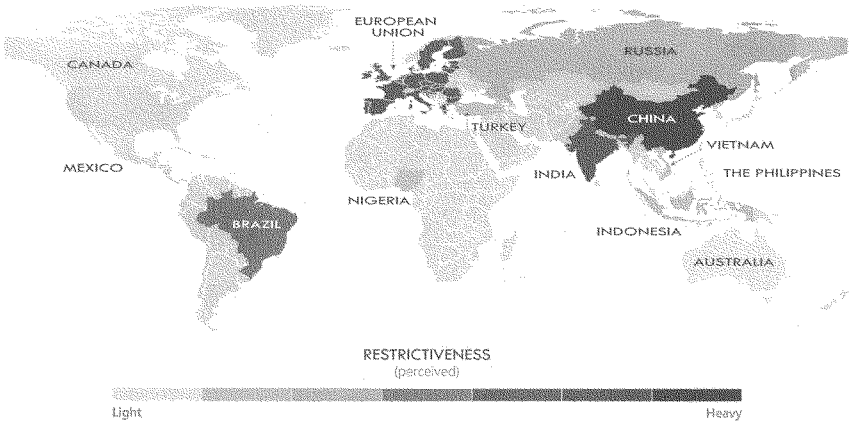
The United States does not take a backseat role to any nation or group of nations in our commitment to personal privacy. At the same time, we should not allow others to unilaterally set a single set of rules for how our citizens and our businesses must operate in the global, digital economy. The U.S. helped create and launch the APEC CBPRs. Today, we must redouble our efforts to advance their cause, secure greater adoption, and show real U.S. leadership – and a true American voice – in the unfolding landscape around privacy, the digital economy and our economic future. This is an essential effort to ensure that digital trade can grow, flourish and advance personal privacy.

The stakes are high; but, with U.S. leadership, the opportunities are immense. We must seize the opportunity to shape the policy landscape around digital trade, and in so doing, to define our future.

Thank you.

Levels of Perceived Digital Trade Barriers in Selected Countries

(based on the U.S. Trade Representative)



RESTRICTIVENESS
(perceived)

Light — Heavy

CRS

COMPETITIVE ENTERPRISE INSTITUTE

Responses to Questions for the Record

Ryan Radia
Research Fellow & Regulatory Counsel
Competitive Enterprise Institute

Before the Joint Economic of the United States Congress

Hearing: The Need for U.S. Leadership on Digital Trade

Question 1: The President's recent announcement of tariffs on Chinese goods were countered by Chinese tariffs on American goods. The President threatens a second round of tariffs. Markets have been spooked by the threat of an escalating trade war.

How would you characterize the magnitude of this trade war against our allies, China and other countries? Is it a tremor or an earthquake?

How likely is it that the administration's trade war on manufactured goods and raw materials will cause collateral damage on U.S. digital trade?

What is the likely effect of the trade war on the small businesses represented by the Chamber?

Response: The Trump administration's recently imposed and announced tariffs are causing worldwide tremors that could lead to major seismic events. Erecting tariff barriers is harmful; erecting them in retaliation to other nations' actions is no less harmful. The presently escalating game of tit-for-tat will benefit no one, but it has created a real risk of collapse in the world trading system that has benefitted consumers around the globe and helped lift billions out of poverty. That would be worse than an earthquake.

With respect to manufactured goods and raw materials, trade is never directly reciprocal, and it is foolish to think of it as such. All political leaders face pressure from different domestic industries to enact protectionist measures, and that pressure tends to come from industries that are uncompetitive at the international level. Given that the United States leads the world on digital trade, it is highly likely that retaliatory measures will be aimed at protecting uncompetitive digital industries in other nations.

America's small businesses are among the casualties of tariffs. Companies adversely affected by tariffs range from Indian Motorcycle in Iowa to Moog Music, a boutique synthesizer company in North Carolina, as well as soy farmers throughout the country—who collectively export $14 billion

in goods to China each year. Tariffs result in harmful consequences ranging from moving production overseas to layoffs to lower demand and idle factory floors.

Question 2: Recent news stories have revealed that corporations like Facebook track and sell an astonishing amount of information about users. This raises questions about privacy.

The European Union's General Data Protection Regulation (GDPR) includes a "right to be forgotten" – the right of individuals to have their personal data erased.

Should Americans also have a "right to be forgotten?" How can we balance individuals' right to privacy with the interests of industry?

Response: Article 17 of the GDPR established a right to erasure, a form of the "right to be forgotten." This requirement, aimed at advancing user privacy, is fundamentally at odds with the freedom of speech guaranteed to Americans by the First Amendment to the U.S. Constitution. As UCLA Law Professor Eugene Volokh explained in a 2000 law review article entitled Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You, "the right to information privacy — the right to control other people's communication of personally identifiable information about you — is a right to have the government stop people from speaking about you." This conflicts with the First Amendment, because forcing a company or person to stop expressing or knowing information "concerning" a data subject is effectively a prohibition on free speech.

A government erasure mandate is not necessary to protect user privacy. Many U.S. technology companies have voluntarily chosen to delete data about a particular user at his or her request. For example, when a user deletes her Facebook profile, data on that user will typically cease to exist on the company's servers after 90 days. Google and Twitter offer similar mechanisms to enable users to delete their data. In competitive Internet markets, firms that fail to offer users a means to delete their data will suffer as privacy-conscious consumers flock to services that make it as easy to leave as it is to join their platforms.

Another concern with the GDPR's right to erasure is that may have the effect of prohibiting blockchain technology. This is because a core aspect of the blockchain is the "immutable ledger," whereby a permanent record is created on the blockchain to ensure the legitimacy of all transactions. This technology has great potential to enhance protection of consumer data on the Internet and foster trust in digital transactions—but the GDPR may result in EU member states missing out on these promising opportunities.

Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM July 17, 2018

To: Representative David Schweikert
Attention: Tiffany Angulo, Legislative Assistant
Attention: Colleen Healy, Joint Economic Committee

From: Rachel F. Fefer, Analyst in International Trade and Finance, rfefer@crs.loc.gov, 7-1804

Subject: **Digital Trade Framework, from Joint Economic Committee Hearing on "The Need for U.S. Leadership on Digital Trade," June 27, 2018**

This memorandum responds to your question raised during the hearing. Your question was:

> I want to also walk through, because my fear is in this discussion it is much more complex than we are actually touching on. You know, whether it is the Europeans' attempt to -- you know, the right to be forgotten, you know, the right to remove data, to how I move a product in a supply chain back and forth, to digital commerce where, what is money? Can I move a cryptocurrency to do a purchase? Can I actually have PayPal, you know, be my mechanisms? Or do I have to touch a SWIFT system that actually has certain bilateral agreements already attached to it, to now to one of my personal fixations is data on supply chains...Am I going the right approach, that part of our issue with Europe is the individual privacy issues, but our issue with certain areas in Asia, it is the control of the money flow and the product supply chain?
>
> ... You know, and within that, we have actually had presentations on you could manufacture a product here, you could actually, you know, use RFID or types of encoded containers, padlocks, to make it much more efficient to move through Customs. We could, you know, the documentation, so it hits Customs; you already had the manifest that completely loads. But that is operating at one level, but now I have a problem if there is privacy on my ability to have made the order, to move the money, to -- was the details in the manufacturing order, was there proprietary information there that doesn't get stolen or handed to the government? Has anyone out there in all of your experience sort of talked about or written about sort of this unified theory of how we deal with Europeans' privacy concerns, parts of Asia's ability to remove money, our concerns about moving IP? I mean, if we came to you and said, "Where do we go to sort of find this unified theory," who has written on it? And sort of a universal question for everyone on the panel.

Given my trade policy focus at CRS, I will address your question from a policy, rather than technical, perspective.

One unifying concept that relates to the issues you mentioned is cross-border data flows. Cross-border data flows are central to crafting approaches that address digital privacy, consumer rights, the Internet of Things, blockchain, crypto-currency, and electronic payments. Cross-border data flows are part of, and integral to, digital trade and facilitate the movement of goods, services, people, and finance. Efforts to impede cross-border data flows may decrease efficiency and other potential benefits of digital trade. For

example, measures to limit cross-border data flows could block the trading of crypto-currency; put personal information or intellectual property at risk if data has to be replicated in multiple locations; or limit the use of blockchain or the Internet of Things to manage supply chains, customs documentation, or electronic payments. Current approaches to cross-border data flows vary significantly across countries, and new restrictions are being put in place in countries such as Vietnam which recently passed a cybersecurity law that requires local data storage.[1] There are various ideas regarding how the United States might approach differing data regimes in other countries. Several groups have written on this topic, including the Information Technology and Innovation Foundation (ITIF),[2] the Brookings Institute,[3] and the McKinsey Global Institute.[4]

Enabling cross-border data flows is a priority of the United States as reflected in the Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114-26), or Trade Promotion Authority (TPA), signed into law in June 2015. Congress included a specific principal negotiating objective for trade agreements "to ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data."[5]

In terms of a holistic or unified theory that encompasses approaches to cross-border data flows and other digital trade policy issues, two policy frameworks you may want to consider are the European Union's (EU) Digital Single Market (DSM) and the U.S. Trade Representative's (USTR) Digital Two Dozen. Each of these frameworks addresses multiple facets of digital trade, from cross-border data flows to cybersecurity.

EU Digital Single Market

The first framework is the EU's Digital Single Market, or DSM. The EU announced its DSM strategy in May 2015 as an effort to modernize and harmonize legislation governing the digital economy across the EU member states. The DSM consists of 16 specific initiatives and multiple legislative proposals and has three broad policy areas:

1. Improving consumer and business access to and efficiency of e-commerce and online goods;
2. Designing rules to support the development of digital networks and services; and
3. Addressing internal trade barriers and building an inclusive digital society with e-government.

The DSM initiatives cover traditional as well as innovative sectors, from telecommunications and audio visual to the Internet of Things and 5G networks. The new EU General Data Protection Regulation (GDPR), which you referred to and was discussed during the hearing, establishes a single set of rules for protection of personal data throughout the EU. The GDPR, along with the draft ePrivacy Regulation that

[1] James Hookway, *Vietnam Tightens Grip on Internet With Data-Storage Law*, The Wall Street Journal, June 12, 2018.

[2] See, for example, Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, ITIF, May 1, 2017; Nigel Cory, *The Global Rise of 'Data Localism'*, ITIF, January 31, 2018; Robert D. Atkinson, Testimony on "International Data Flows: Promoting Digital Trade in the 21st Century," for House Judiciary Committee Subcommittee on Courts, Intellectual Property and the Internet, November 3, 2015.

[3] See, for example, Joshua Meltzer, *The Internet and international data flows in the global economy*, Brookings Institute. May 27, 2016.

[4] See, for example, James Manyika and et al., *Digital globalization: The new era of global flows*, McKinsey Global Institute, February 2016.

[5] P.L. 114-26, Section 102(b(6)C.

seeks to ensure privacy of electronic communications in the digital era, are data protection and privacy-focused initiatives linked to the broader DSM strategy.

The DSM framework has been implemented in a piecemeal fashion, with different initiatives moving faster than others. The European Commission (the EU's executive) has called on the European Parliament and member states (acting in the Council of the EU) to adopt the existing DSM-related legislative proposals, but the process of reaching an agreement is often cumbersome and lengthy and the proposals continue to evolve. While the DSM aims to break down barriers internally in the EU, it does not necessarily promote interoperability or harmonization with other countries or international standards.

Nevertheless, some analysts note that the DSM may set new international standards as other countries imitate EU laws and regulations to ensure access to the EU market. U.S. stakeholders also raise concerns regarding future interoperability with the emerging EU data protection standards and the sustainability of the U.S.-EU Privacy Shield, which currently allows for cross-border data flows between the United States and EU. As noted in my testimony, other concerns related to the GDPR include its complexity, how it is implemented and enforced across Member States and the scale of potential fines.[6]

Digital Two Dozen

The second framework, which addresses some facets of this, is called the Digital Two Dozen. Originally crafted under the Obama Administration and linked to the provisions of the proposed Trans-Pacific Partnership (TPP)[7], the Digital Two Dozen reflects the U.S. view of a set of international rules that promote the free flow of goods, services, and data across a free and open Internet.[8] The 24 principles create a policy framework and could be incorporated into free trade agreement provisions, as was done in the TPP, or as a separate digital agreement with other interested partners.

The principles include an open internet and free flow of cross-border data, non-discrimination between trading partners, protecting intellectual property, protecting consumer rights and privacy, promoting fair competition and innovation, as well as cooperation on cybersecurity. The framework is more comprehensive in terms of scope but less specific than the rules set out in the DSM, and allows a country to implement its own version of rules that align with the framework. Rather than focus on specific technologies or standards (e.g., 5G), it intends to create an environment for innovation and technological advancement and also promotes international standards.

[6] For more information, see CRS In Focus IF10748, *European Union Digital Single Market*, by Rachel F. Fefer and Shayerah Ilias Akhtar, CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick, CRS Report R44257, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, by Martin A. Weiss and Kristin Archick, and https://ec.europa.eu/digital-single-market/.

[7] For more information, see CRS In Focus IF10390, *TPP: Digital Trade Provisions*, by Rachel F. Fefer.

[8] For the full text of the Digital Two Dozen, see https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf.

Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM July 10, 2018

To: Representative Carolyn B. Maloney
Attention: Harry Gural, Senior Policy Advisor
Attention: Colleen Healy, Joint Economic Committee

From: Rachel F. Fefer, Analyst in International Trade and Finance, rfefer@crs.loc.gov, 7-1804

Subject: **Question for the Record: China's Potential to Increase Digital Trade Barriers, from Joint Economic Committee Hearing on "The Need for U. S. Leadership on Digital Trade," June 27, 2018**

This memorandum responds to your question for the record. Your question was:

> In your written testimony, you note that in April 2017, China had almost 720 million internet users – well over double the number in the United States. You also note that China is the world's largest market for retail e-commerce, with over $900 billion in sales in 2016. The Chinese market clearly presents a very large opportunity.
>
> You also describe the ways China actively restricts U.S. digital trade. These include the theft of intellectual property, the so-called "Great Firewall," localization requirements, encryption restrictions, forced technology transfer and failure to enforce intellectual property rights.
>
> It has been extremely difficult to convince China to lower these trade barriers. Let's consider the opposite – how difficult would it be for China to raise these barriers? Is digital trade with China particularly vulnerable because there are so many ways to choke it? How vulnerable are we?

Tensions between the United States and China have grown in recent years over a number of economic and trade issues, and China's policies and actions have limited the ability of U.S. firms to enter or compete in the Chinese market. Today, many U.S. firms are able to access the Chinese market through certain channels, such as utilizing available online platforms, establishing a local presence, or working with Chinese partners. Other U.S. firms are seeking to enter the Chinese market for the first time.

The virtual nature of digital trade could make it vulnerable to a variety of Chinese policies such as limiting cross-border data flows. Looking ahead, it would not be difficult for China to impose further trade barriers and policies as identified in my testimony, making U.S. firms more vulnerable in terms of losing market share or profitability. These include actions by China to:

- Intensify its "Internet Sovereignty" policy and its "Great Firewall," to further block online U.S. market access to Chinese customers;
- Interpret and apply its Cybersecurity Law in a broad manner, including to:

  - Involve safety inspections by the Cyberspace Administration of China (CAC) of foreign technology suppliers that require firms to reveal proprietary source code or other intellectual property to ensure products are "secure and controllable;"
  - Refuse to certify a product due to unspecified risks to national security; or
  - Limit the ability of foreign firms or individuals to use encryption when sending data across borders.
- Increase local content requirements for additional sectors and limits on cross border data flows, limiting consumers' and businesses' ability to utilize external (e.g., U.S.-based) data or services;
- More strictly enforce restrictions on virtual private networks (VPNs);
- Further relax enforcement of intellectual property rights (IPR), potentially leading to increased piracy and IPR theft and discouraging U.S. innovation or deterring U.S. firms from entering the market;
- Direct Chinese officials to steal IP to aid Chinese companies or state-owned enterprises (SOEs) and promote indigenous innovation, including through cyber-theft of U.S. trade secrets;
- Formalize technology transfer policies such as by requiring foreign firms to partner with Chinese companies or SOEs;
- Make licensing and local investment processes for U.S. firms more restrictive, complex or time-consuming;
- Create new rules or regulations to restrict online market access for business-to-business (B2B) or business-to-consumer (B2C) firms, such as language requirements, use of Chinese payment systems, etc.;
- Increase and/or intensify inspections of U.S. exports of e-commerce purchases or of Chinese factories that produce information communications technology (ICT) for U.S. companies; or
- Impose or increase tariffs on U.S. ICT exports.

These actions would impact the digital trade environment for U.S. firms, potentially limiting their ability to grow and profit from the attractive Chinese market. Further limits on market access to U.S. firms could worsen the business climate. Some U.S. firms may exit the Chinese market rather than bear the risks and burdens.

A 2017 U.S.-China Business Council (USCBC)[1] survey found that 40% of companies were less optimistic about the business climate in China compared to 2014; 57% had seen no impact from economic reforms announced four years ago; and technology transfer requirements and IPR protection were cited as acute issues for many U.S. firms.[2] At the same time, Chinese actions limiting the availability of foreign digital goods and services could negatively impact Chinese customers.

In the same vein, a recent Trump Administration investigation determined that "China's acts, policies and practices related to technology transfer, intellectual property, and innovation are unreasonable and discriminatory, and burden U.S. commerce."[3] Subsequent U.S. tariffs and investment restrictions aim, in

[1] The U.S.-China Business Council is a private, nonpartisan, nonprofit organization of approximately 200 American companies that do business with China. For more information, see https://www.uschina.org/about.

[2] U.S.-China Business Council, *2017 Member Survey*, https://www.uschina.org/sites/default/files/2017_uscbc_member_survey.pdf.

[3] U.S. Trade Representative, "USTR Issues Tariffs on Chinese Products in Response to Unfair Trade Practices," March 2018. For

part, to pressure China to reduce digital trade barriers. The Alliance for American Manufacturing voiced support for the Administration's position and stated, "If China doesn't play by the rules, it should lose some of its access to the U.S. market... The administration's proposed actions will help restore some balance with China, as well as recreate an environment where some of the millions of jobs we've lost to China will have a chance of being restored."[4]

However, China has retaliated with tariffs on a variety of imports from the United States and, according to press report, in response to recent and potential U.S. actions, the Trump Administration expects China to take some measures to further impede the availability of foreign goods and services as it cracks down on U.S. businesses.[5]

Finally, it's worth noting that the USCBC, whose mission is "to expand US-China commercial relationship" to benefit its members, called for a "results-oriented dialogue to improve intellectual property protections and market access for American companies in China. The business community wants to see solutions to the issues, not sanctions that would harm families and jobs in each country."[6] The outcome of these developments may further impact the digital trade environment for U.S. firms.

---

more on the Section 301 investigation, see CRS In Focus IF10708, *Enforcing U.S. Trade Laws: Section 301 and China*, by Wayne M. Morrison.

[4] Alliance for American Manufacturing, "China Must Play Fair Or Face Consequences," April 3, 2018.

[5] Wendy Wu and Laura Zhou, "Get ready for short-term trade pain, U.S. tells American companies in China," *South China Morning Post*, July 1, 2018.

[6] U.S.-China Business Council, "USCBC Statement on President Trump's Decision Regarding Investment Restrictions," June 27, 2018.

July 10, 2018

Questions for Ambassador Robert Holleyman from Representative Carolyn B. Maloney
(June 27, 2018)

The "nuclear option"
In the growing trade war, China has reacted symmetrically to the administration's actions – countering tariffs with tariffs. But there is no reason to assume that it could not retaliate in other ways.

For example, what would happen if China pursued a "nuclear option" – by further reducing enforcement of intellectual property rights? How badly would this affect digital trade?

The most likely way in which China may retaliate – beyond tariffs – is through an indirect means that would hurt U.S. companies doing business in China. For example, such indirect means could be through delayed approval processes, new and unexpected administrative processes, or through direct or subtle messages for Chinese consumers to avoid purchasing U.S. products. For many U.S. companies currently selling successfully or wishing to expand in the Chinese domestic market, the threat of indirect retaliation is a real risk.

China may reduce or slow enforcement of intellectual property rights, although this is likely to be subtle if it happens. China wants to be seen publicly as supporting intellectual property rights, and many Chinese domestic industries want intellectual property protection enforcement. While it remains to be seen, in practice, the Chinese government could minimize protections or selectively enforce IPR rights in a way that undermines U.S. interests.

All of this could adversely affect digital trade, as the focus would shift away from this important space, and thereby slow or distract from important reform and market-opening efforts. At the same time, China has a very restricted market when it comes to opportunities for U.S. companies to succeed in digital trade in China. Restrictions on data flows, as well as restrictions on foreign investment in Internet, cloud-computing and data-related sectors, are real barriers to the growth of digital trade and the ability of non-Chinese companies to compete within China. The U.S., along with its allies, must continue to focus on opening those markets and breaking down existing barriers.

Cybersecurity
Our financial services industry depends on its ability to assure customers that our systems are secure. In an increasingly digital world, rock solid security is a selling point. A reputation for security generates profits and economic growth.

The private sector has made cybersecurity a high priority. What can the federal government do to help ensure that our digital products are the most secure in the world?

The federal government can help ensure that our digital products are the most secure by continuing to enable innovative encryption and other mechanisms to be used and incorporated into products. Periodic calls for "back-doors" in security technologies must be resisted as they could be exploited by hackers and nation states. The federal government should also support more information sharing with the private sector, which is an essential partner in combatting a growing number of security threats. Additionally, the U.S. should support funding for research, education and training for cybersecurity professionals.

The U.S. government should be a role model in elevating the importance of cybersecurity within government systems and in helping the public understand the important role of enterprises and individual citizens in deploying and updating secure products. Together with its allies, the U.S. must fight against protectionist measures in countries that seek to require U.S. and global companies adopt domestically-

produced security products. The inherent risk of mandating use of domestic security products is that vulnerabilities may be exploited or best-of-breed security configurations may be forced to change to meet protectionist domestic requirements.

Privacy

Recent news stories have revealed that corporations like Facebook track and sell an astonishing amount of information about users. This raises questions about privacy.

The European Union's General Data Protection Regulation (GDPR) includes a "right to be forgotten" – the right of individuals to have their personal data erased.

Should Americans also have a "right to be forgotten?" How can we balance individuals' right to privacy with the interests of the industry?

The GDPR has generated considerable attention since it entered into force and has, of course, has broad potential penalties attached. In practice, however, it is still too new to fully grasp what the real-world impact will be as the EU implements the new standards. Governments, companies, and other stakeholders are still watching to see what the practical effects will be for citizens, companies, and other organizations involved in the commerce and the privacy debate in Europe, and beyond. The U.S. Congress should look again at enacting a comprehensive federal privacy law, particularly now that some U.S. states, such as California, are adopting legislation to fill in gaps in current U.S. law. In that context, European practices in areas like the "right to be forgotten" – while laudable for their strong defense of individual liberties – should be considered and can be better understood in relation to their impact, practical effect and public interest considerations. And regulators should seek approaches that strike an appropriate balance between all of these. Broadly speaking, we should not assume that a European approach to privacy is the best or even a desirable approach in all areas – particularly given that the impact and real-world implications of the GDPR are only just yet starting to be felt.

What we do know, however, is that there is an approach to privacy that the United States has endorsed in the context of our participation in the Asia Pacific Economic Cooperation (APEC) forum. The APEC Privacy Framework and the APEC Cross-Border Privacy Rules (CBPRs) provide a flexible model for protecting personal privacy and enabling data flows within the Asia-Pacific region. They recognize that national governments will insist on adopting privacy frameworks that meet their domestic needs. The U.S. should expand our support and advocacy for adoption and implementation of the CBPRs among the APEC economies. This Asia-Pacific system is intended to be interoperable with the European approach, as manifest most recently through the GDPR. For the broadest and best protection of privacy, the U.S. should lead with our domestic laws, continue to advance and promote the APEC CBPRs, promote inclusion of consumer privacy principles in our trade negotiations, and push back against instances where privacy may be a disguised barrier to trade. Privacy protection is a fundamental element of ensuring trust and confidence in digital trade. The U.S. can and must lead in this effort.