Statement of the U.S. Chamber of Commerce

ON: The Dynamic Gains from Free Digital Trade for the U.S. Economy

TO: U.S. Congress Joint Economic Committee

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

DATE: September 12, 2017

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 3 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 this opportunity to testify on behalf of the U.S. Chamber of Commerce in order to address the dynamic gains from digital trade for U.S. economy as well as the barriers American companies are facing abroad. I am Sean Heather, vice president of the Chamber's Center for Global Regulatory Cooperation (GRC).

Digital trade has proven to be transformative and will continue to impact how Americans interact with one another, work, and do business. The global economic impact of the Internet was estimated to be $4.2 trillion in 2016, making it the equivalent of the fifth-largest national economy.[1] The benefits of the digital economy are not limited to "technology" companies but are experienced by companies across all industries from agriculture to manufacturing. In fact, three quarters of the value created by digital trade accrues to more traditional firms utilizing digitalization, such as manufacturers, retailers, and banks. U.S. businesses of all sizes rely on the Internet to manage their relationships with customers and supply chains; digital commerce has spread widely and is even creating completely new industries. Across all sectors, digital trade has increased US employment by up to 2.4 million jobs.[2]

The United States has positioned itself as the leader of the global digital economy. As a result the United States stands as the world's leading producer of digital services and content. American companies innovate faster and generally out-compete foreign firms. In 2015, exports of information and communications technology (ICT) services accounted for $65 billion of total U.S. exports while potentially ICT-enabled services exports made up $399 billion, driving a significant digital trade surplus.[3]

However, our leading position is not assured as certain governments actively seek to disadvantage American technological innovation. In order to enable continued economic growth at home, we must develop a common agenda to maintain and strengthen America's role in the global digital economy. This hearing is an important step in setting that agenda.

The digital economy is dependent on the movement of data. Foreign governments are endeavoring to forcibly create their own "Silicon Valleys" by implementing policies on the movement of digital goods and services that serve as regulatory barriers that limit digital trade, cross-border data flows, and market access. Such a flawed approach to economic development, rooted in protectionism, not only obstructs American companies' ability to do business in foreign markets, but it also fails to deliver the promises of the digital economy to economic growth in foreign markets.

In contrast, a liberalized approach to digital trade adopted globally benefits American and

---

[1] Paul Zwillenberg, Dominic Field, and David Dean, Greasing the Wheels of the Internet Economy, Boston Consulting Group, February 2014, https://www.bcgperspectives.com/content/articles/digital_economy_telecommunications_greasing_wheels_internet_economy/ .

[2] United States International Trade Commission, Digital Trade in the U.S. and Global Economies, Part 2, https://www.usitc.gov/publications/332/pub4485.pdf

[3] Alexis N. Grimm, Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT Enabled Services, BEA, May 2016,http://www.bea.gov/scb/pdf/2016/05%20May/0516_trends_%20in_us_trade_in_ict_serivces2.pdf

foreign business alike by allowing the increased uptake of technology and the ability to safely and seamlessly move data. In fact, a study commissioned by the U.S. Chamber of Commerce found that reducing market and regulatory barriers to cross-border ICT services could produce $1.72 trillion in global GDP gains.[4] Such actions could also generate billions of dollars in potential new government revenues, millions of new jobs, and hundreds of thousands of new businesses.[5]

Cross-border data flows

Cross-border data flows are 45 times higher than they were in 2015, now outpacing global flows of trade and/or finance. The dramatic increase in cross-border data flows is enabling goods and services to be traded more easily, by more people. This is encouraging as global flows of information and data of all types support economic growth. By some estimates, over the course of a decade, global flows acting together have raised global GDP by 10.1%, with the value amounting to some $7.8 trillion in 2014 alone. Digital flows – which were barely in existence 15 years ago – accounted for $2.8 trillion of that impact,[6] and digital flows now have a larger impact on GDP growth than the global trade in goods.[7]

Data localization requirements are becoming more prominent and problematic, limiting the ability of companies to move data. The movement of data through the global economy is becoming just as important as the ability to move goods, services, or capital. Further benefits will not be realized if data does not have the ability to cross borders. Data localization requirements directly limit the movement of data. Some common requirements U.S. companies are facing include mandatory establishment of a data center or physical presence within a jurisdiction in order to operate as well as restrictions on how data can be transferred internationally.

The Chamber has been actively working to eliminate and prevent forced localization requirements. Over 36 countries currently have data localization policies limiting the movement of different types of data ranging from financial to telecommunications data. Such requirements severely hinder the ability of U.S. companies to operate in these jurisdictions, while limiting choices and driving up costs for their consumers, and ultimately reducing their competitiveness.

---

[4] The U.S. Chamber of Commerce commissioned Spire Research and Consulting to create a model in order to quantify the economic impact of full liberalization of cross-border ICT services and rules globally by creating an open, competitive marketplace. In order to better demonstrate that both end users and providers are winners in an open ICT services environment, the study examines a group of eight globally important markets from a diverse range of economic development, including Brazil, the European Union, Indonesia, Japan, Korea, Nigeria, Turkey, and Vietnam. Our findings demonstrate across the board benefits. Access report here: https://www.uschamber.com/report/globally-connected-locally-delivered-the-economic-impact-cross-border-ict-services

[5] Ibid.

[6] James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, March 2016, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

[7] Ibid.

The government of Indonesia has ten different pending regulations that would require data to be stored locally or restrict its movement. For example, Kominfo/MICT Regulation No. 82/2012 requires U.S. companies to establish both data centers and disaster centers within Indonesia. Indonesia also has a draft regulation on "over-the-top" (OTT) services, services provided over the Internet, which requires companies to establish data centers within Indonesia and maintain a local presence in Indonesia.

Russia's data localization laws are severely limiting the ability of U.S. companies to operate within its borders as well. Federal Law 242-FZ requires data collected on Russian citizens to be stored in data centers located in Russia. This has forced both U.S. firms operating in Russia or providing services from the U.S. to rewire their operations, consider exiting the market, or buying server space in Russia to provide the same services at a higher cost.

Localization policies are only increasing. France and Germany, in particular, have been edging toward more and more policies that force the storage of data in-country. The French government has invested in and promoted the use of a "le cloud souverain" (sovereign cloud), which is only open to French companies operating their services directly in France. While approaches to localization vary by region in Germany, at the federal level Germany passed the Telecommunications Act, which went into force July 1, and now requires telecommunications metadata to be stored locally.

Local Content Requirements

Foreign governments are mandating the use of local content in an attempt to boost the local economy, enhance skills and capabilities, and boost employment. Local content requirements are increasing worldwide with more than 146 active measures documented in 39 countries in 2015.[8] As the Chamber's *Globally Connected, Locally Delivered* study demonstrates, such requirements hinder long-term growth by lowering productivity, increasing prices, and diverting investment. The Chamber believes that open, competitive marketplaces are more likely to accelerate local economic growth.[9]

China and Russia have encouraged indigenous innovation through local content requirements, particularly linking specific requirements to government procurement contracts and standards. For instance, Russia grants preferential treatment to domestic ICT companies when considering government procurement contracts. China's standards, such as its "secure and controllable" standard, could potentially force companies to use domestic intellectual property and encryption processes. In 2016 alone, China introduced more than 30 measures across various industries, including ICT-specific standards. Over 80 jurisdictions have created new ICT-related technical standards, many of which are not consistent with global standards and

[8] Cathleen Cimino-Isaacs and Jan Zilinskey, Local Content Requirements: Backdoor Protectionism Spreading Under the Radar, Peterson Institute For International Economics, July 2016, https://piie.com/blogs/trade-investment-policy-watch/local-content-requirements-backdoor-protectionism-spreading

[9] U.S. Chamber of Commerce, Globally Connected, Locally Delivered: The Economic Impact of Cross-Border ICT Services, 2016, https://www.uschamber.com/report/globally-connected-locally-delivered-the-economic-impact-cross-border-ict-services

norms. These types of standards create a hodgepodge of sometimes conflicting and overlapping standardization requirements that disrupt global supply chains.

Data Protection

As the movement of data increases, protecting privacy has become a growing concern around the globe. More than 95 jurisdictions currently have data protection legislation passed, up from around 70 jurisdictions in 2014.[10] Around 68 of those jurisdictions with data protection regulations already in place are busy considering updates and revisions to their legal frameworks.[11] While privacy standards are necessary in order to ensure consumer protection, consumers and businesses also need to be able to move and access data. However, governments often enact data protection measures that interfere with these needs without a good regulatory justification, creating difficulties for companies conducting business in-country and worldwide. It is important to note that these challenges are not necessarily traditional "trade" type problems where trade tools are well situated to tackle concerns. More often these issues require intensive engagement on the part of U.S. regulators engaging in regulatory cooperation type activities.

A good illustration of this type of concern is over the implementation of the EU's General Data Protection Regulation (GDPR). GDPR will come into force in May 2018, and companies are expected to be in full compliance by then. Yet, guidance from data protection authorities has been slow to come out, and many U.S. and European companies still have a number of compliance questions. Consistent implementation of GDPR across all EU member states represents an immense regulatory challenge for the EU that has consequences for EU competitiveness in the digital economy in addition to American firms doing business there.

Many Latin American countries have turned to Europe and are using GDPR as a template for creating their own privacy regime. For example, Brazil currently has three draft data protection bills pending, all based on the GDPR model. Many other pending regulations across Latin America include stipulations on international data transfers that could serve as significant barriers to digital trade. Not all of these bills provide a list of countries whereby international data transfers are permitted, but those that do have not always included the United States as adequate to receive transfers. The shortcomings of the 'adequacy' approach to privacy underscore the need for new, more flexible approaches to protecting privacy on a cross-border basis - including through the APEC Cross Border Privacy Rules, as discussed in more detail below.

While privacy regimes can create regulatory challenges that impede digital trade, the motives aren't always easily discernable to label them clear attempts to obfuscate trade commitments. Many countries have cited privacy concerns as the basis for requiring foreign companies to store data within national borders. Yet, as studies have shown, forcing data to be

[10] Kate Lucente and James Clark, Data Protection Laws of the World, DLA Piper Global Law Firm, January 2017, http://blogs.dlapiper.com/privacymatters?s=handbook.

[11] International Conference of Data Protection and Privacy Commissioners, Census 2017, September 2017, https://icdppc.org/.

stored locally does not have any incremental impact on increasing privacy.[12] Instead, such policies increase risks to privacy and security by requiring storage of data in a single centralized location that is more vulnerable to outside intrusion.[13] In these instances, privacy regulations become forced localization requirements and a traditional "trade" type problem.

Cybersecurity

Digital trade also raises new challenges and opportunities related to cybersecurity. Many countries are already reviewing existing cybersecurity regimes. Like new data protection regulations, U.S. companies face the challenge of differing regulations throughout the world as well as new security policies that hold the potential to masquerade protectionist motives. The Chamber believes the best way to address cybersecurity concerns are through voluntary risk-management, investment, and information sharing. Collaboration between government and industry is critical. While the Chamber recognizes that there is no one-size-fits-all approach, there are a growing number of cybersecurity policy concerns in the international arena.

Specifically, China's recent cybersecurity law requires review processes for a broad but unclear scope of industries that could potentially to be used to impede market access, extract concessions, and advance industrial policy. The uncertainty and overlapping requirements created by this new law will hinder the ability for U.S. companies to do business in China. China's emerging legal and regulatory frameworks governing information technology pose serious challenges for global connectivity. Cloud computing and other digital technologies that require a seamless flow of data are already changing the nature of numerous industries, including manufacturing. Yet, Chinese efforts to exert greater control over where commercial data is stored and how it is transferred are skewing the decision-making process for companies that must decide where products are made and innovation takes place.

In the EU, the recently finalized Network Information Security (NIS) Directive will come into effect in May 2018. Under the NIS Directive, Member States will introduce new laws and adapt existing requirements. It is important that these new regulations are implemented in a reasonably consistent and efficient manner. In particular, U.S. companies could benefit from Member State consideration of how to incorporate existing foreign cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, into implementation of the NIS Directive. This understanding is particularly important as the NIS Directive, similar to GDPR and data protection law, could become a template for future cybersecurity legislation around the world.

Intellectual Property Protection

The innovation and technology that drives U.S. competitiveness and makes American companies leaders relies upon intellectual property protection and the legal frameworks that

[12] Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, Localization Barriers to Trade: Threat to the Global Innovation Economy, The Information Technology & Innovation Foundation, September 2013 http://www2.itif.org/2013-localization-barriers-to-trade.pdf?_ga=1.126836941.1580072294.1483722057

[13] Leviathan Security Group, Value of Cloud Security, 2015, http://www.leviathansecurity.com/cloudsecurity

govern such rights. Effective protection of patents, trademarks, copyrighted works, and trade secrets (to include proprietary algorithms) optimizes the availability of, and access to, creative and innovative products and services in digital trade. Moreover, IP-intensive industries account for 45.5 million American jobs, $6.6 trillion in GDP, and 52 percent of all U.S. exports, according to the U.S. Department of Commerce.[14]

Too often forced localization measures are designed to require tech transfers as the price to gain entry to a foreign market. When this occurs, American companies' competitive advantages are reduced as strategic "know how" is handed over to cultivate and aid domestic competitors. Further, countries are increasingly restricting intellectual property rights by introducing new requirements around local production, procurement and creation of digital content.

Copyright piracy and trademark infringement, too, represent well-documented drains on the competitiveness of American companies that produce propriety software, entertainment content, and branded products enjoyed around the world.

The U.S. Chamber's International IP Index (the "Index") illustrates the wide divergences among countries in the quality of protection afforded copyrightable works and trademarks in global digital trade.[15] For example, of the 45 economies benchmarked in the latest edition of the Index, only 5 received full scores for the availability of frameworks that promote cooperative action against online piracy, and only two — not including the United States — were recognized for having adequate availability of frameworks that promote action against the online sale of counterfeit goods. In addition, as illustrated in the Index, the majority of economies lack rules to promote cooperative action against online piracy, such as limitations on liability for Internet service providers that cooperate with copyright owners to remove infringing content.

Having a sound legal framework that protects intellectual property and includes enforceable sanctions is critical to consumer confidence and safety. Additionally, it is important for the development of high quality digital products and services as well as supporting the delivery of such products and services through sophisticated, accessible platforms.

Emerging Technology

Finally, as more traditional products and services connect and depend on data to function, it is important that a holistic view is adopted around the policies impacting emerging technologies. Blockchain, wearables, drones, and autonomous vehicles are just the beginning of the possibilities that these relationships could forge. Emerging technologies are creating new interdependencies between developers, providers and users. In fact, 68 percent of American

[14] Intellectual Property and the U.S. Economy: 2016 Update, U.S. Patent and Trademark Office, accessed March 29, 2017, https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf

[15] The U.S. Chamber International IP Index is a comparative intellectual property law study and an industry standard for benchmarking intellectual property rules and practices. The current edition, "The Roots of Innovation," published in February 2017, benchmarks IP rules in 45 economies against 35 indicators in six categories: Patents; Copyrights; Trademarks; Trade Secrets and Market Access; Enforcement; and International Treaties. Access the full index here: www.uschamber.com/ipindex

voters say technology will make their communities operate better.[16]

However, foreign regulators and policymakers are increasingly pushing to regulate emerging technology by attempting to anticipate potential worst-case scenarios. This type of approach, in a modern economy dependent on the ability to quickly access data and digital products and services, will forestall innovation and fail to fully meet societal goals. Furthermore, these new technologies require coordination on existing issues, such as infrastructure, skills, privacy, security and liability, in order to reach the marketplace.

The Internet of Things (IoT) is rapidly expanding, connecting humans with technology to improve their lives and increase the efficiency of industrial operations. It is estimated that there will be more than 50 billion connected devices by 2020, over 30 times the number in 2009.[17] Employing one-size-fits-all standards for connected devices does not seem the right match to confront face-paced commercial demands and risks that companies face online. Yet, the European Union is expected to recommend "measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber secure"[18] this month. Premature regulations will place unnecessary burdens on industry, especially small and midsize enterprises, driving up the cost of devices while offering no greater security. Different sets of flexible cybersecurity best practices will be necessary for different IoT audiences, ranging from producers and network operators to users.

Many countries as well as the International Telecommunication Union (ITU) are also looking to push further burdensome and outdated regulations on OTT services and applications. When a foreign government indicates their intent to regulate OTTs, they are often seeking to apply legacy regulations, such as requiring partnership agreements between American OTT players and local operators. These regulations threaten technologies that have become a key driver of growth in the global economy including texting; video sharing; cloud and IoT services; money transfers; and mobile payments. The proposed regulations in countries such as Indonesia and Vietnam, will weaken the global innovation ecosystem, inhibit investment in entrepreneurs, slow job creation, constrain this new source of overall economic growth, and erect unnecessary obstacles to international trade.

Instead of focusing on regulation, policymakers and regulators should seek to enable innovation and investment to ensure users are able to benefit from increased use of emerging technologies. Therefore, an appropriate and successful regulatory approach should focus on balancing critical societal objectives with the benefits to consumers. Unnecessary and unproven regulation only serves to stifle innovation and investment, dampen competition, and harm consumers.

---

[16] U.S. Chamber of Commerce Technology Engagement Center (C_TEC) http://ctecintelligence.com/

[17] Dave Evans, Cisco, April 2011, The Internet of Things: How the Next Evolution of the Internet is Changing Everything. http://bit.ly/1LgfMSb

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee on the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy, May 10, 2017. http://bit.ly/2pvCoUG

Recommendations

Given the economic importance of digital trade to the United States, it is crucial that the U.S. government create a policy agenda that maintains and strengthens U.S. leadership of the digital economy. To ensure this, we recommend the follow actions:

Prioritize digital issues in active trade and investment policy agenda – The Chamber supports a U.S. policy agenda that seeks commitments from our trading partners to foster the cross-border movement of digital goods, services, and information. The U.S. government should prioritize digital issues in its trade agenda and ensure they receive sustained, high-level attention by the Office of the United States Trade Representative and other relevant agencies.

Secure strong digital trade commitments from other countries to:

- Ensure the ability for U.S. businesses in all sectors to move data across borders by prohibiting the forced localization of data;
- Prohibit measures that link market access and other commercial benefits to local technology infrastructure;
- Prohibit customs duties on electronic transmissions, including information being transmitted electronically;
- Prohibit discrimination against U.S. technology companies, products, and/or services;
- Prohibit burdensome OTT regulations that extend legacy regulatory and licensing requirements to online services and applications;
- Prohibit the transfer or access to software source code or algorithms as a condition for market access;
- Facilitate a regulatory environment that allows companies to utilize data collection and analysis;
- Streamline and expedite customs processes, through the use of electronic customs forms, electronic signature and authentication, electronic labeling, and secure on-line payment;
- Modernize de minimis rules, which allow low-value goods to enter into a country duty free under a simplified entry process;
- Include appropriate and effective safe harbor mechanisms for intermediary liability; and,
- Champion smart and effective approaches to encryption that do not require companies to undermine product security.

Develop an enforcement agenda – It is important that we not only advocate for digital trade in our agreements but also create and utilize enforcement mechanisms to ensure compliance. For example, South Korea was required to change its regulatory approach of restricting data flows and outsourcing of financial data as a result of the U.S.-Korea (KORUS) Free Trade Agreement. South Korea's implementing regulation fell short of removing these barriers. Through consultative and enforcement mechanisms created under KORUS, the U.S. government and South Korea were able to discuss these issues resulting in a revision of the South Korean system in 2015. Today, South Korea has one of the most open data flows regimes in the world, though some unjustified restrictions remain in such areas as maps data. The

Chamber supports statements made by Commerce Secretary Wilbur Ross that the United States should consider which tools are appropriate to address digital trade barriers such as intellectual property theft and forced technology transfers.

Continue supporting international privacy frameworks – The United States should continue to support vehicles such as the EU-U.S. Privacy Shield Framework and APEC Cross Border Privacy Rules (CBPRs) that promote the movement of data between borders and bridge national privacy regimes. Workable arrangements are increasingly needed between the U.S. and key trading partners. The U.S. government should also look for opportunities to promote adoption of the APEC CBPRs and develop similar privacy frameworks with other interested partners. These frameworks allow U.S. companies to reliably transfer data and signal the United States' and its partners' commitment to strong, interoperable privacy protections. They create cost effective and dependable means for data transfer, allowing U.S. companies to channel resources into creating new jobs, innovation, and better serving their customers.

Ensure trade-facilitating approaches to cybersecurity across the world – It is important that the rise of cyber regulation does not undermine trade, but instead safeguards the data flows that underpin it. The NIST Framework for Improving Critical Infrastructure Cybersecurity is an innovation-friendly framework encouraging technology-neutral approaches to managing cyber risks. The United States should work with international policymakers to align IoT security programs with industry-backed approaches to risk management, such as the NIST framework. The United States should also work with partners to create common cyber incident reporting structures and forums through which public and private stakeholders can voluntarily share cyber threat information.

Utilize Department of Commerce and State Department digital attaché programs – These programs should be used to drive U.S. competitiveness internationally by promoting U.S. digital exports and advocating for the adoption of U.S.-friendly digital regulatory frameworks. As the eyes and ears on the ground, these attachés can provide U.S. companies with on-the-ground expertise and assistance while also proactively working with local governments to prevent policies that may harm digital trade.

Actively engage in shaping foreign regulation – U.S. regulators play an important role in outside trade agreements by seeking opportunities to coordinate with foreign regulators. They should continue to work with our trading partners through new and existing dialogues to collaborate with foreign regulators enabling U.S. companies to compete on a more level playing field internationally.

This includes engagement in international forums such as the Organization for Economic Co-operation and Development, the World Trade Organization, and ITU, who are endeavoring to increase their influence in creating international digital trade norms and rules. Many countries are using these forums as an opportunity to push burdensome and harmful regulations on American companies that will harm their operations abroad.

Conclusion

I thank the Committee for the opportunity to testify today, and I look forward to a robust discussion on opportunities and barriers to digital trade. Digital connectivity has allowed American companies to experience faster revenue growth, productivity, and innovation. Technology has been an underutilized tool that can help U.S. government increase competitiveness, drive economic growth, and create jobs. The Chamber and its members look forward to engaging with you further to advance the benefits of digital trade for all Americans.

Attachments to Testimony

I would like to submit the following along with my statement:

1. *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*
   https://www.uschamber.com/sites/default/files/021384_BusinessWOBorders_final.pdf
2. *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies*
   https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf
3. *Globally Connected, Locally Delivered: The Economic Impact of Cross-Border ICT Services*
   https://www.uschamber.com/report/globally-connected-locally-delivered-the-economic-impact-cross-border-ict-services
4. *IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership*
   https://www.uschamber.com/sites/default/files/uskbc_iot_2016_paper_final.pdf
5. *International IP Index*
   http://www.theglobalipcenter.com/ipindex2017/
6. Letter to European Commission on EU NIS Directive
   https://www.uschamber.com/sites/default/files/documents/files/industry_comment_ltr_to_european_commission_on_future_of_public_private_partnerships.pdf
7. Letter to National Institute of Standards and Technology on Information on Current and Future States of Cybersecurity in the Digital Economy
   https://www.uschamber.com/sites/default/files/u.s._chamber_letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf
8. *Made in China 2025: Global Ambitions Build on Local Protections*
   https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf
9. *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*
   https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf
10. *Seeking Solutions: Attributes of Effective Data Protection Authorities*
    https://www.uschamber.com/report/seeking-solutions-attributes-effective-data-protection-authorities
11. *Transatlantic Cybersecurity: Forgin a United Response to Universal Threats*
    https://www.uschamber.com/TransatlanticCybersecurityReport
12. *Vital & Growing: Adding up the US-Indonesia Economic Relationship*
    https://www.uschamber.com/sites/default/files/documents/files/vital_and_growing_-_adding_up_the_us-indonesia_economic_relationship.pdf