ITI

Written Testimony of

John S. Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy
Information Technology Industry Council (ITI)

Before the

Committee on Foreign Affairs

U.S. House of Representatives

U.S. Cyber Diplomacy in an Era of Growing Threats

February 6, 2018

Written Testimony of
John S. Miller
Vice President for Global Policy and Law, Cybersecurity and Privacy
Information Technology Industry Council (ITI)

Before the
Committee on Foreign Affairs
U.S. House of Representatives

U.S. Cyber Diplomacy in an Era of Growing Threats

February 6, 2018

Chairman Royce, Ranking Member Engel, and Distinguished Members of the Committee on Foreign Affairs, thank you for the opportunity to testify today. I am John Miller, Vice President for Global Policy and Law, Cybersecurity and Privacy at the Information Technology Industry Council (ITI), and I am pleased to testify before your committee today on the important topic of assessing U.S. cyber diplomacy, including the State Department's cyber functions, in an era of growing threats. As we survey the global cyber policy landscape, we agree we are living in a time of remarkable global cyber policy activity, signifying both opportunity and risk. While it's instructive to understand where the policy landmines representing those risks are currently located and how they can undermine the United States government's (USG's) cyber policy objectives, global cybersecurity efforts, and the competitiveness of U.S. companies, it's also important for us to seize the opportunity presented by this global uncertainty to advance cyber policies that promote the cross-border data flows underpinning competitiveness, economic growth, and security. We welcome your interest and engagement on this subject.

ITI[1] represents over 60[2] of the world's leading information and communications technology (ICT) companies. Cybersecurity and cyber policy more broadly are rightly a priority for governments and our industry, and we share common goals of improving cybersecurity, protecting the privacy of individuals' data, and maintaining strong intellectual property protections. Further, our members are global companies, doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across the full range of global industry sectors, such as financial services, healthcare and energy. We thus acutely understand the impact of governments' policies on innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. Our members have extensive experience working with governments around the world

[1] **About ITI.** ITI is the global voice of the tech sector. We advocate for global public policies that advance innovation; open access to new and emerging markets; promote e-commerce expansion; drive sustainability and efficiency; protect consumer choice and privacy, and enable the transformational economic, societal, and commercial opportunities that our companies are creating. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, internet companies, and companies using technology to fundamentally evolve their businesses. ITI's diverse membership and expert staff provide a broad perspective and intelligent insight in confronting the implications and opportunities of policy activities around the world. Visit http://www.itic.org/ to learn more. Follow us on Twitter for the latest ITI news @ITI_TechTweets.

[2] See ITI membership list at http://www.itic.org/about/member-companies.

on cyber or digital policies. In the technology industry, as well as other global sectors, when discussing any cyber policy, it is important to consider our connectedness, which is truly global and borderless.

Taking a global approach is at once our top priority and challenge, because policymakers don't necessarily look at these issues through the same lens as global companies – many understandably refract cybersecurity, for instance, through their sovereign rights and obligations to protect their territories and their citizens. Unfortunately, doing the equivalent of building policy walls at your borders in the name of better security doesn't work in the digital world – from either a business or technical perspective – and may have the unintended consequence of doing more harm than good.

I will focus my testimony on four areas: (1) demonstrating the critical importance and interrelatedness of cross-border data flows to the top cyber policy issues our companies grapple with every day; (2) illustrating how some of the top global cyber policy trends put global data flows, security, and our companies' competitiveness at risk; (3) positioning recent U.S. cyber policy activity within this global context; and (4) offering recommendations on the path forward, including discussing how the policies expressed in the *Cyber Diplomacy Ac*t (H.R. 3776) can help advance our collective cyber policy interests.

Cross-Border Data Flows and the Top Cyber Policy Issues Facing the ICT Sector

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows to the ICT sector and the global economy, and the centrality of data to many cutting-edge technologies and innovations, such as the Internet of Things (IoT), Artificial Intelligence (AI) and big data analytics. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers, to securing global networks and the personal data of customers across the globe. With data increasingly at the center of not only the global economy but our lives, securing that data, and protecting privacy of individuals' data, is of paramount importance to ITI's companies, and the data-driven innovations mentioned above are increasingly critical to our shared cybersecurity mission as well.

In addition to facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for global companies, helping to secure the systems and networks that manage production schedules and Human Resources data, as well as to communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is also necessary to enable a seamless and secure internet experience for hundreds of millions of citizens around the globe.

I suspect the top "buckets" of cyber policy issues facing ITI's companies – international trade and data flows; standards and regulations; privacy and data protection; and cybersecurity – are the same issues facing most companies doing business in the global, digital economy. And so it's not surprising that all these issues implicate data flows in one way or another.

Data Flows and International Trade. We think of these issues together, because for our companies these issues are inextricably linked. There is no trade in the modern, global digital economy without the ability to move data across borders – transferring data, communicating data, storing data, and of course protecting data are all fundamental to digital trade. Cross border data flows are fundamental to businesses of all sizes, and in all geographies, as well as to the key innovations that will drive the future, such as IoT and AI. The value of cross border data flows to e-commerce and digital trade cannot be overstated, and indeed there are plenty of statistics we can cite placing the aggregate dollar values of cross-border data flows between the U.S. and any number of trading partners in the hundreds of billions of dollars with the overall value of such data flows involving the U.S. topping $6 trillion in 2014.[3] It is important to note these numbers are so large because the impacts involve much more than just the U.S. ICT sector – here in the U.S., or in countries proposing or adopting protectionist measures. The ICT sector is a horizontal enabler of services trade across all sectors of the economy. A recent study by UNCTAD – the United Nations Conference on Trade and Development – found up to 75% of the benefits of e-commerce impact other sectors of local economies. Misunderstanding of this fact amongst developing countries is palpable, as policies designed to "grow a domestic ICT sector" will have much broader negative impacts, as businesses in developing economies such as Brazil and India will not be able to grow and operate on a global scale without the ability to move data across borders.

Standards and Regulations. Trade associations representing global businesses are often characterized as "anti-regulation" – and of course, it's true that not a lot of businesses go out of their way to ask to have regulations imposed on them. However, when we survey emerging standards and regulations globally, the bigger problems often aren't necessarily the standards and regulations themselves, but the fact that many countries are contemplating *local* standards, and *local, siloed* regulatory approaches. The proliferation of siloed technical standards, regulations and localized data and security requirements could impede the seamless functioning of the internet and global digital economy as we experience it today. Multiple country specific standards, or requiring that non-domestically sourced equipment undergo differing security requirements, can lead to the balkanization of the global digital infrastructure, threatening the continued interoperability of the innovative technologies that have fueled the internet's growth. The potential negative impacts of forced localization and other protectionist measures become even more pronounced when we factor in potential impacts on the cloud, Big Data, IoT, and emerging technologies such as AI.

Privacy and Data Protection. We all acknowledge that exponentially more data is being generated than ever before. Unlike natural resources, data is an infinite resource because we create it, and then data itself is leveraged through a host of innovative technologies that help unlock its value. Whether we are talking about Big Data Analytics, IoT, AI – data is at the center of all these innovations. Given data is at the center of trade and innovation, securing that data, and protecting the privacy of that data, is of paramount importance to governments, companies and citizens alike, to protect consumer privacy and to enable secure transactions. Governments around the world are aware of this as well, and many are examining, re-examining, or considering privacy and data protection laws for the first time. But data protection policies that seek to protect data by, for instance, restricting its cross-border transfer by requiring a determination of whether the receiving country's laws are "adequate," or preventing data from leaving a country's borders entirely by requiring that it be stored on domestic servers, can not only prevent future innovative uses of data, but may prevent us from realizing a host of socioeconomic uses that data helps us realize , in areas such as health, agriculture, finance, and cybersecurity.

Cybersecurity. Cybersecurity is often the rationale lurking behind many of the problematic policies that threaten data flows, such as data localization policies, proposed requirements for in-country security

[3] See *Digital Globalization: The New Era of Global Flows*, McKinsey Global Institute, March 2016, available at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

testing, audits or assessments, or requirements for domestic manufacturing or server locations. The net result of such policies will likely be a slowing or diminishing of cross border data flows, which will in turn negatively impact global e-commerce development and growth. However, what is sometimes overlooked is that data flows are of central importance to cybersecurity itself. U.S. and global ICT companies have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them better protect their own systems and maintain high levels of security for customer data, IP and the technology ecosystem as a whole. Indeed, one of the preeminent cyber policy achievements in the U.S. in recent years – the 2016 passage of a bipartisan cybersecurity threat information sharing legislation[4] – was intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity. So, it's critical to understand that the trend of impeding data flows generally is also contrary to the thrust of current U.S. cybersecurity policy and threatens to undermine progress to better secure the global digital ecosystem and economy.

Top Global Cyber Policy Trends

The policy issues described above manifest themselves in various global cyber policy trends, sometimes alone but oftentimes in combination. After briefly discussing these trends, I will highlight the current state of play in a few major economies to help illustrate the pervasiveness of today's "global policy threats."

Forced Localization. Forced localization refers to a broad set of policies that are designed to compel companies to relocate all or part of their global business operations within a country's borders. Data localization is a prime example: foreign firms could be required to process data at a national datacenter, purchase or manufacture locally, or transfer intellectual property to a domestic competitor as a precondition for market access. We've seen localization proposals popping up almost everywhere over the last few years – and while such measures today have become increasingly complex, often they are designed to achieve a straightforward goal: impeding the ability of foreign companies to compete with local firms in providing goods, services, and technologies in global business transactions. While many governments view these policies as helping them to meet the challenges of a complex global economy, the truth is the drawbacks for a country and its citizens far outweigh the benefits. Instead, localization efforts work to reduce the competitiveness of countries who employ them across all economic sectors and undermine the health of the global economy by raising the cost of doing business internationally.

While much of the discussion of forced localization policies has appropriately focused on data localization, in fact forced localization policies can take many forms, including:

- *Data Localization*: Requirements that companies store, process, or otherwise handle data within a country's borders. This includes restrictions on the free flow of information across borders that underpins an open internet.
- *Local Content Requirements*: Mandates that a certain amount of the final value of a good or service be sourced domestically, either by purchasing it from local companies or by manufacturing or otherwise producing or providing it locally.

[4] *Cybersecurity Information Sharing Act of 2015*

- *Technology Transfer Requirements*: Measures requiring businesses to transfer proprietary intellectual property directly to local competitors or through government agencies.
- *Local Presence Requirements*: Requiring a company to establish a local office in-country or provide goods or services using local facilities, infrastructure, or agents, etc.
- *Standards and Conformity Assessment*: Requirements to comply with unique, non-global technical standards, or to conduct duplicative or overly restrictive conformity assessment procedures without recognition of international norms that make current technology and new innovations possible.
- *Indigenous Innovation Requirements*: Requirements to use or impose a preference to domestically developed technology.
- *Domestic Employment Requirements*: Requirements to achieve a certain level of domestic employment.

The proliferation of forced localization measures is a trend that the world's leading economies – including the U.S. – - must work hard to combat if policymakers want to continue to leverage the internet to spur innovation, job creation, and economic growth. Given that localization policies are out of step with the international norms and policy frameworks that have guided innovation in technologies and the rapid rise of technology-enabled industries, the rise of such policies in recent years should be cause for concern.

ITI has conducted an in-depth survey of forced localization policies worldwide. While half of localization measures are acknowledged by governments as having a naked economic objective, such as local ICT sector development, in nearly half of the cases ITI has studied there are noneconomic rationales or objectives, often security-related, lurking behind these policies.[5]

There is a certain irony in security being cited as a driving rationale in roughly one-third of the forced localization cases ITI studied – such policies may negatively impact security itself. As noted above, there is a security rationale underlying many of the proposed localization regulations, and few would question the sovereign right of nations to pursue cybersecurity or other regulations that will legitimately protect their national security. However, in our view many of these proposed security requirements, while well intentioned, are grounded in a fundamental misconception – that location of manufacture or the country of origin of an IT product is somehow dispositive of the security of that product, or that the location of data or restricting its flow guarantees stronger protections.

In fact, geographic-based restrictions are simply not a reliable way to create better security. Fundamentally, product security is a function of how a product is made, used, and maintained, not by whom or where such products are made. Geographic-based restrictions not only ignore the reality that most supply chains for IT products are global, but run the risk of creating a false sense of security for any countries who advocate for such provisions to advance their national cybersecurity interests. At a time when greater global cooperation and collaboration is essential to improve cybersecurity, restrictions

[5] ITI's 2015 research indicated security-related objectives behind roughly one-third of forced localization laws, with national security cited as the primary objective 22% of the time, and government access to data for law enforcement or national security purposes cited 9 % of the time. Privacy/data protection was the stated objective behind governments' forced localization policies in an additional 13% of the cases we studied. So, while relatively transparent protectionism is clearly driving a good chunk of these problematic laws, the full picture complicated by noneconomic factors such as security and privacy.

based solely on geography risk undermining the advancement of global best practices and consensus-based standards for cybersecurity, such as secure development lifecycles.

Siloed or Country-specific Standards and Regulations. Countries are increasingly proposing regulations or standards that are country specific, rather than grounded in international standards or approaches – whether we are talking about privacy-based transfer restrictions or security-based testing requirements. Different requirements across countries pose significant regulatory fragmentation risks. The negative impacts of regulatory fragmentation include the inefficiencies associated with companies potentially being required to adopt a separate privacy and security compliance program for every country they do business in, and pose significant challenges to global interoperability due to varying technical or legal requirements. Layer on top of that sector specific laws within these countries, competing overlapping regulations (e.g., competing security incident notification and data breach notification), or multiple levels of government regulators potentially getting into the mix (e.g., Brazil's financial regulator promulgating security regulations for banks), and it's easy to see the potential problems in this area.

Cybersecurity Audits, Assessments and Testing Requirements. Efforts by policymakers to "measure," "certify," "test" or "label" for cybersecurity – e.g., the EU's proposed ENISA Regulation urging the development of a security certification Framework, or India's Department of Telecommunications proposed implementation of local security certification and testing requirements for telecommunications equipment – show no signs of abating. While these and other policy proposals are wide ranging, at their core is a common set of underlying concerns regarding the trustworthiness and security of ICT products, supply chains and systems. While determining how best to use cybersecurity measurements to drive increased accountability for cybersecurity across organizations is unquestionably a worthwhile goal, global proposals seeking to impose certification, audit or assessment requirements on private entities are often invasive in that they contemplate such tests being conducted by government auditors or assessors, thus requiring access to companies' source code or other proprietary information. Further, the testing contemplated often involves local standards, rather than global standards. A better approach to driving accountability via measurement is espoused by Draft 2 of Cybersecurity Framework Version 1.1, which emphasizes the role of measurement as a tool for self-assessment and internal use by organizations, rather than as intended for external use by policymakers or regulators to evaluate or judge the sufficiency of organizations' cybersecurity risk management programs.

Application of Legacy Regulations to Technology and Services Innovations. Of emerging concern are the attempts to "retrofit" legacy regulations to technology and services innovations in a manner that that would impact broad swaths of the internet economy, or have unintended consequences on innovation, security, or other dimensions of cyber policy. Two recent examples of this trend involve the rise of "OTT" regulations, and the expanding use of export controls.

The Rise of "OTT" Regulations. Numerous foreign governments are seeking to subject U.S. online services and applications to burdensome legacy regulations designed to address the particular technical and market characteristics of traditional telecommunications or broadcast providers. These measures – often vaguely called "Over-the-Top" or "OTT" regulations in foreign markets – take different forms globally. What they increasingly require is that online services register as telecommunications or broadcasting providers, contribute to universal service funds, comply with local content quotas and make subsidy payments, guarantee a particular quality of service, establish local presence and/or local data storage, and implement technical mandates, including certain emergency calling requirements that are not technically feasible or economically reasonable. These regulations are creating market access barriers for U.S. services, including in China, Colombia, the European Union and several EU member states, Ghana, India, Indonesia, Kenya, Thailand, United Arab Emirates, Vietnam, and other countries.

Extension of Export Controls to Cybersecurity Products. Another troubling regulatory trend that appears on the rise is the extension of export controls to cybersecurity technologies. During the 2013 Wassenaar Arrangement plenary session, the member nations agreed to implement export controls related to intrusion detection software and IP network communications surveillance items. While the human rights concerns underlying the controls were laudable (i.e., protecting activists from monitoring by authoritarian governments and keeping software and technology out of the hands of hackers who could use it maliciously), the controls as originally agreed to were overbroad, sweeping in virtually any type of software, hardware, and technology designed to counter "intrusion" software. The 2013 controls were also ineffective in achieving their intended objective of barring companies from exporting specific tools to specific end-users for specific purposes, were divergently applied across Wassenaar signatories, and from the perspective of most would have undermined U.S. and global cybersecurity efforts.

The good news is that many of the flawed aspects of the 2013 controls were improved pursuant to the outcomes of last year's Wassenaar plenary session, but the risks of further expansion of export controls to other cybersecurity technologies, or other technologies that could negatively impact either cybersecurity efforts or global data flows more broadly, remain. For instance, the European Union is currently in the process of redrafting its Dual-Use Export Regime, implicating many of these same issues.

These issues are not hypothetical – they are both very real and pervasive, insofar as they are not really limited to particular countries, regions or economies. I provide a "deep dive" on how these issues arise in several major markets below.

China. ITI members continue to be concerned with market access issues in China, especially barriers to entry portrayed as security justifications. China's discriminatory Cybersecurity Law (CSL) creates a legal framework that institutes multiple and overlapping security review regimes for foreign technology with limited transparency and significant ambiguity that can easily preference domestic industry. The security review regimes under the CSL and related measures compel companies to disclose sensitive information. The Law also contains "secure and controllable" requirements, which were raised in USTR's 2017 and 2016 National Trade Estimate (NTE) reports as a known issue with serious implications for domestic preferences. Moreover, the scope of the CSL is broad and several of its provisions remain ambiguous, conditions that will lead to problems with compliance.

Data localization measures have dramatically increased in China, jeopardizing not only the technology industry, but all other industries that depend on ICT platforms for global operations. Barriers that pre-dated the CSL already cost U.S. services billions of dollars as companies were pushed out of the market, with a vast majority of U.S. companies describing Chinese internet restrictions as either "somewhat negatively" or "negatively" impacting their capacity to do business there.[6] For instance, even though U.S. cloud service providers (CSPs) have stimulated innovation and application of cloud computing

[6] According to ITI member survey conducted in September 2016.

technologies around the world, China has imposed several onerous regulations on U.S. CSPs – effectively barring them from operating or competing fairly in China. Chinese laws and regulations on non-Chinese CSPs can force U.S. CSPs to transfer valuable intellectual property, surrender use of their brand names, and hand over operation and control of their businesses to Chinese companies in order to operate in China.

Embedded within the Cybersecurity Law and among numerous regulations and standards are requirements to store, process, or manage data locally within China and restrictions on flows of data in and out of China. The most prominent restrictions are found in the *Measures on Cross-Border Data Transfer* and the *Critical Information Infrastructure Protection Regulation*. The CSL creates additional barriers by mandating data localization for CII network owners and operators in China and restricting flows of data out of China.

These measures directly affect the ability of many industries beyond the tech sector to conduct normal business operations. This trend toward increased control over where and how data is transferred represents a destructive and misguided attempt to protect Chinese tech companies from foreign competition. Taken together, these measures pose great costs to U.S. firms in all sectors.

China also continues to flout international standards and norms, as demonstrated by an increase in laws and standards that include China-specific requirements. In April 2017, the State Encryption Management Bureau released the draft Encryption Law, which currently requires unique encryption of products and services within China that does not align with the Common Criteria.[7] The draft would also impose an intrusive licensing scheme covering the sale, use, and import or export of commercial cryptography that poses significant risks of disclosure for companies. Meanwhile, the draft Standardization Law causes concern among companies for its potential to create a burdensome standards regime. In establishing a framework for standards-making, the draft Standardization Law contains unclear definitions of standards types and their status as mandatory or voluntary. Numerous Chinese standards that are categorized as voluntary continue to be regarded by Chinese government agencies as mandatory or de facto mandatory, a problem that the law has not adequately addressed.

Beyond the negative impacts on U.S. companies in terms of access to the Chinese market itself, perhaps most worrisome is the potential of the CSL to emerge as the dominant approach to cyber policy in the region, or even globally.

India. India presents a unique case, insofar as the U.S. and India in 2016 successfully negotiated a bilateral agreement, the Framework for the U.S.-India Cyber Relationship, that seems to run counter to many of the problematic policies India continues to pursue.

In May 2017, India's Telecommunications Engineering Centre (TEC) proposed changes mandating certification and local testing for all telecom products regulated under India's Telegraph Rules. These changes are set to begin in October 2018 and include a wide range of technical requirements from electromagnetic compatibility (EMC) and safety to security testing and IPv6 interoperability, as well as environmental requirements, among others. TEC and the Department of Telecommunications (DoT) have not provided a rationale or details on the implementation this broad certification framework, nor have they notified it to the WTO Technical Barriers to Trade Committee for global stakeholder feedback.

[7] Common Criteria is the technical basis for the Common Criteria Recognition Arrangement (CCRA), an internationally-employed technical certification and mutual recognition agreement for secure IT products.

Many of these requirements will likely be redundant with existing international testing and certification of telecom products. Moreover, India has little capacity to or infrastructure to implement these changes. ITI and local industry are asking TEC/DoT to pare back the initial scope of the requirements and ITI is seeking clarification on many outstanding issues before TEC/DoT move ahead. ITI is also urging the authorities to follow global best practices and accept international test reports and certificates when applicable, and to allow for additional consultation with industry and an adequate transition time.

DoT also continues to pursue a mandate that telecom companies, operating networks within India and overseas, put in place necessary systems to ensure the networks within India's geographical borders comply with telecom security rules. In April 2013, DoT identified certain telecom products to be screened at an authorized test lab, of which some were singled out as "high risk items" to be checked from October 1, 2013. DoT notified industry that all imported telecom and ICT products (if internet connected) will have to be locally tested by DoT-accredited labs even if such devices have been screened by private labs within the Common Criteria Recognition Arrangement (CCRA) alliance. However, since notifying this requirement, DoT has delayed implementation every year since due to a lack of capacity for testing and unclear requirements for implementers. This measure, if ever implemented, would impose significant costs to U.S. companies exporting to India, and yearly last-minute delays in implementation have created significant uncertainty for companies exporting to India.

India maintains and is expanding local preferences for government procurement. Historically, the most prominent measure—*Preferential Market Access for Government Procurement (PMA-G)*—has steadily expanded from low level computing systems to high end servers and other technology products. This measure, implemented by MEITY and DoT, requires products to have certain levels of local content in order to qualify for procurement price preferences, effectively blocking many American companies from competing. However, in June 2017, the Department of Industrial Policy and Promotion released a new "Make in India" Order which gives a 20% price preference to all products with 50% Indian local content in government procurement. As a result, both MEITY and DoT are updating their PMA-G policies to reflect this order, expanding both the scope and effect of their policies. In addition, MEITY recently released a notification that will expand this program to cybersecurity products – a sector in which the U.S. has a significant competitive advantage. These requirements are extremely problematic for American tech companies that wish to do business in India, and the expansion on PMA to cybersecurity products is particularly problematic to the extent it necessarily impacts companies' intellectual property rights. When implemented, ITI member companies would be unable to compete fairly for government ICT contracts, which make up a large portion of the Indian ICT market.

In addition, the Telecommunications Regulatory Authority of India (TRAI) has published several consultation papers on a range of issues (cloud computing, machine to machine communications, data protection, and more). Though few concrete steps have yet been taken as a result of these consultations, many of them have explored potentially damaging policy options – most notably data localization and extending telecommunications regulations to OTT service providers. The outcomes of these consultations warrant attention from the USG as they could result in restricting the ability of U.S. companies to export their services to India in the future.

Russia. Russia has adopted several forced localization policies and laws. Federal Law 242-FZ, which requires data collected on Russian citizens to be stored in Russia, came into effect on September 1, 2015. This law affects the normal business operations of all industries in Russia by imposing inefficient operational rules, particularly the requirement in Article 18 to store personal data concerning Russian citizens in data centers located in Russia. It appears that Roskomnadzor, the federal regulator responsible for implementation, has accepted mirroring of data—keeping copies of data within Russia rather than the more extensive requirements of processing it in-country—to be compliant with the law. However, the vague language in the law could allow for blocking cross-border data flows in the future, lending to an uncertain business environment in Russia. Furthermore, even mirroring of data can be very costly to businesses, particularly Small and Medium Size Enterprises (SME), increasing barriers to entry for the Russian market. In addition, the federal media regulator has been empowered to block local access to the websites of non-compliant companies. Given the law's expansive scope, foreign companies without a legal presence in Russia, which might pay only a cursory attention to the Russian market, can be labelled data protection violators and blocked. In late 2016, Russia began conducting audits and fining companies for violations. In one high profile case, this audit resulted in a U.S. internet company being blocked outright from doing business in Russia.

In January 2016, the Kremlin issued a 16-point plan for improving the competitiveness and security of the Russian ICT sector through import-substitution, increased surveillance capabilities, and increased education on issues related to cyber. The plan is focused on import substitution and has generally been talked about in the context of "internet sovereignty." Two new executive decrees associated with this plan call for ministries to create plans that prioritize Russian-produced software and equipment for government purchases, create additional obligations for how the personal information of Russian citizens is processed, regulate the encryption of data, reorganize federal cyber-threat monitoring, and establish a Center of Import Substitution for Information and Communication Technologies. In October 2016, a bill was introduced in the Duma that would further require government entities to provide preferences even to Russian developed software that is based on foreign-developed middleware. Further implementation and follow-up decrees have been opaque and seemingly poorly coordinated, so there is little information on how the plan has progressed.

Federal Law No. 149-FZ "*On Information, Information Technologies and the Protection of Information*," as amended in 2014, has two particularly troubling elements. First, Article 10.1 "*The Duties of an Organizer of Dissemination of Information on the Internet*," requires "organizers of the distribution of information on the internet" to retain all metadata within Russia for six months and provide access to that data to security agencies. This applies to an incredibly wide range of companies that facilitate the receipt, transmission, delivery, and/or processing of electronic messages—including any email and internet-based messaging services. Second, Article 10.2, the "Blogger's Law," requires bloggers with more than 3,000 daily users to register with Roskomnadzor and places restrictions on what they can and cannot post to their websites. This law not only has significant free speech and human right implications, but it also creates costly barriers for U.S. companies who wish to do business in Russia.

Lastly, on July 7th, 2016 President Putin signed a package laws (374-FZ and 375-FZ) that amended Russian Federal Laws 126-FZ and 149-FZ—known as the "*Yarovaya Amendments.*" These amendments require "organizers of information distribution on the internet" to store the content of communications that they enable within Russia for six months. In addition, telecommunications companies must store metadata of all communications within Russia for three years, whereas "organizers," referring to internet providers, must store metadata for one year. If any of this data in encrypted, then companies must also provide encryption keys to the implementing agency, the Federal Security Service (FSB). These requirements will be incredibly costly for companies operating in Russia, so much so that domestic telecommunications companies have been in vocal opposition to the law, a rare event in the country.

European Union. There are also a range of policy and regulatory proposals related to security and privacy in the EU that potentially jeopardize data flows.

E-Privacy Regulation. The European Commission unveiled its draft proposal for an ePrivacy Regulation (ePR) last year. The ePR is a priority issue for ITI and our members for several reasons, including the broad material, definitional and territorial scope of the proposed regulation's reach, prescriptiveness of its provisions, size of contemplated penalties/fines, and inefficiencies and confusion caused by overlap and conflict with the GDPR. While it is hard to single out just a few concerning provisions, perhaps most troubling of all is simply the vast scope of electronic communication services (ECS) data the draft proposes to regulate – the "Regulation applies to any exchange of information using electronic communication services and public communications networks, including content and metadata," and expressly applies not only to OTTs but communications among IoT devices, including machine-to-machine communications, and thus directly impacting three of the leading edge data-driven innovations. As for the penalties, fines for violations of the ePR can range as high as the greater of €20M, or 4% of worldwide revenue. ITI has also pointed out potentially problematic unintended consequences of the ePR on cybersecurity, particularly on the ability of companies to retain third party cybersecurity providers to defend their networks due to rigid consent and other requirements. ITI will continue to advocate for changes to ePR to minimize the impacts on important emerging technology priority areas such as artificial intelligence, OTTs and IoT.

Safe Harbor Invalidation and Privacy Shield. Most are aware the transatlantic trade relationship was legitimately placed in serious jeopardy back in 2015, when the invalidation of the Safe Harbor agreement by the Court of Justice of the European Union (CJEU) ruling in *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14) ("*Schrems*") cast uncertainty on the ability of companies to transfer data from the EU to the U.S. While the U.S.-EU Privacy Shield arrangement, which took effect on August 1, 2016, and was recently reaffirmed by the European Commission following the first joint annual review of the agreement, represents a strong commitment by both the U.S. and EU to enable transfers of data across the Atlantic and safeguard consumer privacy, threats to transatlantic data flows remain due primarily to two factors: 1) the pending judicial review at the European Court of Justice of standard contractual clauses, which give U.S. companies an alternative option to ensure that they can transfer data from the EU to the U.S., and 2) challenges in other EU courts to the Privacy Shield itself.

EU Cybersecurity Measures. The Network and Information Security Directive (NIS Directive), the first EU-wide cybersecurity legislation, must be transposed into member state law by May 2018, and the threat of siloed approaches (across the member states) to implementation on key issues, such as the scope of NIS application to technology companies and the potential of asymmetric security incident notification requirements (including rationalizing them vis-a-vis the GDPR's data breach notification requirements), remains. While Germany's legislation implementing NIS is already largely in place, and the UK (who is implementing NIS despite its impending departure from the EU due to Brexit) released their draft legislation to transpose the Directive late last year, several other member states have yet to release legislation to transpose or implement NIS at all, making it hard to fully gauge the risks of regulatory fragmentation. In the latter part of last year, the European Commission also released a comprehensive "cybersecurity package" including a revision and update of the 2011 Cybersecurity Strategy and Proposal for a Regulation on ENISA (the EU Agency for Network and Information Security), the "EU Cybersecurity Agency," and on information and communication technology cybersecurity certification (the "Cybersecurity Act").[8] Key issues of concern with the proposals include the overbroad and potentially far-reaching scope of the cybersecurity certification scheme, the potential for it to be linked to EU rather than international standards, and the current lack of ENISA resources to support its vastly expanded mandate.

Recent U.S. Cyber Policy Activity in the Global Context

On balance, recent cyber policy activity in the U.S. acknowledges both the importance of global data flows and avoids many of the policy pitfalls identified above. *The Cyber Diplomacy Act of 2017* (CDA) helpfully recounts many of the noteworthy cyber policy initiatives advanced or supported by the U.S. over the past several years that are not only supportive of data flows, but necessarily depend on prioritizing and resourcing international approaches to address our shared cyber challenges, including:

- 2011 U.S. International Strategy for Cyberspace
- 2016 International Cyberspace Policy Strategy
- 2016 Commission on Enhancing National Cybersecurity
- Multilateral declarations at the G-7 and G-20
- May 2017 Executive Order on Cybersecurity (EO 13800)

To that list, I would add the Framework for Improving Critical Infrastructure Cybersecurity (the "**Cybersecurity Framework**"), a voluntary, risk management framework grounded in international standards and best practices that was co-developed by NIST and other USG stakeholders in partnership with industry, and the *Cybersecurity Act of 2015*,[9] bipartisan **information sharing legislation** expressly designed to increase the flow of information for cybersecurity purposes. Additionally, some of the initial outputs spurred by the **EO 13800**, including the **botnet report**,[10] similarly acknowledge the importance of the international dimension of cyber policy.

All these policies, spanning both the Obama and Trump Administrations, implicate ecosystem-wide, global cyber challenges calling for global solutions advanced via international and public-private partnerships and collaboration.

The Cyber Diplomacy Act of 2017. The CDA is a welcome and complementary contribution to this recent body of U.S. cyber policymaking that appears to strike the right chord on multiple fronts. Of particular note are the following elements of the bill:

Taking a Global Approach That Promotes Data Flows, Innovation, Openness and Economic Prosperity. The CDA's expression of the overarching policy objectives it is trying to achieve fairly encapsulates the types of cyber policy approaches that help promote data flows, innovation and economic prosperity, and that ITI routinely promotes: *"Congress declares that it is the policy of the United States to work internationally with allies and other partners to promote an open, interoperable, reliable, unfettered and*

[8] See Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

[9] Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N (2015).

[10] See NTIA's Draft "Report to the President on Enhancing the Resilience of the internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" at: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

secure internet governed by the multistakeholder model which promotes human rights, democracy, and rule of law, including freedom of expression, innovation, communication, and economic prosperity, while protecting privacy and guarding against deception, fraud and theft." (Sec. 3(a))

Securing and implementing commitments based on cyber policy norms. The CDA prioritizes several commitments to pursue to advance cyber policy norms that would help mitigate the problematic global policies detailed earlier in my testimony, including:

- Furthering cross border data flows by prohibiting localization
- Incentivizing security by design
- Shielding critical infrastructure entities and CERTS from state-sponsored attacks
- Avoiding state-sponsored IP theft to provide commercial advantages to the private sector

Actionable and accountable agreements. The CDA also smartly seeks to establish guardrails designed to make those agreements both actionable and accountable. The CDA compiles a list of existing **bilateral cyber agreements** with nine countries. Over the past several years The Department of State and other key USG stakeholders such as the Departments of Homeland Security (DHS) and Commerce have done an admirable job of forging a series of cyber bilateral agreements consistent with the governing principles articulated above. As the CDA points out, however, there is a need to follow through by making "evidence-based assessments" regarding the functioning of those agreements, to make sure our counterparties are fulfilling their commitments and other obligations**. Multilateral agreements** are also a clear part of the solution to furthering international progress on cybersecurity and other cyber policy issues, and the bill acknowledges important foundational work that has already been done at the G7 and G20. This is one area, perhaps, where the CDA could more specifically call out the need for actionable and accountable follow through, as it does explicitly in the context of bilateral agreements.

Prioritizing and Allocating Department of State Resources. Realizing the international cyber policy objectives expressed in the bill will require adequately prioritizing and allocating sufficient resources, including regarding the Cyber Coordinator role at the State Department.

The CDA proposes the Department of State cyber coordinator should be a Senate-confirmed position at the rank of ambassador. This makes good sense for several reasons. First, the rank and title of the position sends an important message to other countries regarding the importance the USG places on the cyber issues falling within the coordinator's purview. Second, the practical reality is whoever resides in this position will often have to negotiate with counterparts at other countries holding a similar rank – these counterparts need to know they are dealing with a peer with proportionate decision-making authority. Finally, staffing the position at a senior level can aid in interagency discussions with peer decisionmakers at DHS, Commerce and other USG stakeholders, and can help provide greater continuity through subsequent administrations and personnel changes.

The scope and scale of cyber issues facing the U.S. and the Department of State is growing - we urge that the cyber coordinator's office be adequately resourced to handle this mandate. As the next wave of emerging technologies and digital innovations continue to take hold, cyber issues will only continue to grow in breadth and prominence as policy, economic and security issues for the United States, and the Department of State's lead cyber official and office should be adequately resourced to handle them.

Recommendations

My testimony thus far should make clear there are landmines all over the global cyber policy landscape. While it's instructive to understand where they are, and the stated and unstated motivations underlying them, what's more important for the USG is defining and resourcing a collaborative, proactive strategy, in partnership with the private sector, to drive forward the admirable policy objectives expressed in the CDL. Ultimately, helping that global, open, innovation-friendly approach gain traction will be the best way to influence those countries at earlier stages of cyber policy development in a direction that supports the policy objectives shared by the USG and industry – not simply because we support them, but because those are the policies that will ultimately help developing countries fulfill their internet-fueled economic and digital aspirations.

Below are concrete recommendations for USG actions internationally that can help improve global data flows, security, and the other international cyber objectives expressed in the CDA.

Continue to Prioritize and Resource International Cybersecurity Standardization. To counter the trend of various countries increasingly advocating for their own local security standards, testing protocols, certifications, etc., it seems obvious the U.S. needs a proactive and adequately resourced national strategy involving both industry and government working together to develop and further international cybersecurity standards, consistent with the policy expressed in the CDA. The U.S. has already made some progress in this area, including the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (the "International Standardization Strategy") published by NIST in 2016. We recommend that the current administration prioritize furthering this strategy to improve the U.S. government's participation in the development and use of international standards for cybersecurity, as well as IoT, AI and other emerging standards areas. Doing so will require a unity of effort with industry, as well as adequate resources and political support.

Further the Cybersecurity Framework Approach Globally. The Cybersecurity Framework approach represents the most prominent counterweight to many of the data-restrictive policy approaches recounted above and that are growing in prominence globally. The Framework leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. The Framework has also consistently been lauded for providing a common language to better help organizations comprehend, communicate and manage cybersecurity risks – it can serve as a common language for global policymakers as well. International Cybersecurity Framework alignment is essential to its longevity, and foundational to driving such alignment involves the global Framework promotion efforts of both industry and government. Promoting the Framework in its current form will help the U.S. to sustain its leadership on cybersecurity around the world, and this will in turn help to further enhance the Framework's use within the United States. To facilitate further global adoption, USG stakeholders should promote the Framework approach with their global counterparts. For example, the Department of State should reference the Framework in its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. ITI has also urged NIST to explore, with industry stakeholders, the opportunity for submitting relevant parts of the Framework as an international standard. The latest draft of the Roadmap to Framework Version 1.1 indicates NIST has actively engaged with the ISO and IEC to map existing international standards to the Framework, work that has led to the anticipated publication of an ISO/IEC Technical Report.

Leverage Multilateral Fora to Drive Cyber Policy Solutions. Multilateral agreements are also a clear part of the solution to furthering global progress on cybersecurity and other cyber policy issues, and the CDA references important foundational work that has already been done at the G7 and G20. While not all multilateral fora hold equal promise, ultimately pursuing multilateral solutions in parallel with bilateral ones can be an important force multiplier to drive policy solutions across the global digital economy. For example, good progress has been made at the Asia-Pacific Economic Cooperation (APEC) forum to further the Cross-Border Privacy Rules (CBPRs) framework. The APEC CBPRs are flexible enough to be adopted on a broad scale and are gaining traction across a diverse set of economies in the APEC region, providing a mechanism to move data safely between organizations while providing a bridge to address variations in laws or regulatory fragmentation amongst the participating economies. The United States, Mexico, Canada, Japan, South Korea, Singapore, the Philippines and Australia are already participating or have committed to participate in the CBPRs, and other APEC economies have signaled their interest in joining. The CBPRs offer a scalable system that holds the potential to be less burdensome to economies and companies than navigating other more restrictive, burdensome, resource-intensive, data transfer mechanisms.

Conclusion

Members of the committee, ITI and our member companies are pleased you are examining the role and importance of cyber diplomacy in a world of evolving and increasingly sophisticated threats. Unfortunately, government policymakers globally are increasingly responding to the expanding sophistication and capabilities of cyber adversaries and more frequent and severe cyber incidents by proposing cyber laws and policies that can create trade barriers for U.S. companies and threaten to impede cross-border data flows. If left unchecked, this activity threatens to undermine both the trust and interoperability undergirding the global digital ecosystem.

Historically, the U.S. has maintained a leadership position in cyberspace – from the companies who have led the way in building the global digital economy and internet-based services that have fueled its growth, to visionary cyber policy developments such as the Cybersecurity Framework, to pioneering bilateral cyber agreements negotiated with allied and competitor nations alike. If the USG aspires to maintain its leadership position going forward, it must not only work collectively – both domestically and on the global stage, bilaterally and multilaterally, via public-private collaboration and across sectors – but it must lead.

ITI stands ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to collectively advance cyber policies that promote global data flows, innovation, security, economic prosperity, and the other laudable objectives expressed in the *Cyber Diplomacy Act*.

I thank the Chairman, Ranking Member, and Members of the Committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.