U.S. CHAMBER OF COMMERCE

July 17, 2018

Via iipp2-18@ntia.doc.gov

Ms. Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, DC 20230

Subject: International Internet Policy Priorities

Dear Ms. Alexander:

The U.S. Chamber of Commerce appreciates the U.S. Department of Commerce's National Telecommunications and Information Administration's (NTIA) recognition of the importance of the internet and digital communications to U.S. innovation, economic competitiveness, prosperity, education, and civic and cultural life, as well as the determination to identify priority issues for 2018 and beyond. The Chamber welcomes this opportunity to provide input and recommendations to help effectively shine a light on the barriers American companies face in delivering digital products and services.

The benefits of the digital economy are not limited to technology companies but are spread widely across manufacturing, agriculture, and services. To stay competitive, American businesses need to continue harnessing the power of technology at home and abroad. Increasingly, however, countries are erecting arbitrary barriers that make it more difficult for U.S. businesses to operate.

The Chamber fosters and encourages partnership between industry—across sectors—and U.S. government partners at home and abroad to drive solutions to help prevent and lessen the impact of international policy divergence. Economic competitiveness and innovation thrive in an Internet ecosystem that is smartly regulated; fosters data flows; embraces international competition and open markets; protects data and intellectual property; prioritizes Internet access, consumer choice, and good governance; aligns to industry-supported international standards; strengthens cybersecurity and resilience; modernizes customs for the digital era; and encourages cooperation and accountability among governments.[1]

[1] U.S. Chamber of Commerce. *Global Digital Policy Declaration.* https://www.uschamber.com/issue-brief/global-digital-policy-declaration

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

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

***

NTIA's request for comment captures four themes for its international internet policy priorities, which the Chamber captures here for the purposes of commenting:

Open Markets and the Free Flow of Information: The ability to seamlessly move data across borders and access information is arguably as important to an economy today as the movement of capital. Virtually no company, regardless of sector, can do business, let alone export goods or services, without the ability to move data and access information across borders. Too many countries are erecting barriers to obstruct data flows, offering a false choice in achieving regulatory objectives at the expense of data movement.

Data localization requirements can emerge in a variety of regulations from banking to cybersecurity. Regardless, all of them directly limit the movement of data by creating the mandatory establishment of a data center or physical presence within a jurisdiction in order to operate as well as restrict how data can be transferred internationally. Such requirements create an uneven playing field by severely hindering the ability of U.S. companies to operate in these jurisdictions, while limiting choices and driving up costs for consumers and ultimately, reducing competitiveness.

In addition to localization barriers, American industry is becoming the target of new taxation proposals, which could act as *de facto* tariffs.[2] Increasingly countries, for example, the European Union and Chile, are looking to implement a tax on digital services, which will disproportionately affect U.S.-based companies. The Chamber would prefer a solution that is agreed to at the international level, such as within the ongoing work of the OECD, to reform how companies are taxed, rather than indiscriminately targeting the revenues of "digital services," which are poorly defined in existing proposals.

The Chamber continues to work actively in order to eliminate and prevent forced localization requirements in several jurisdictions:

[2] Huffbauer, Gary and Zhiyao (Lucy) Lu. Peterson Institute for International Economics. Policy Brief. *The European Union's Proposed Digital Services Tax: A De Facto Tariff*. June 2018. https://piie.com/system/files/documents/pb18-15.pdf

Brazil: The government is considering a proposed regulation, Complementary Norm 14, which would regulate how government and procurement data is stored in the cloud and would require that data, metadata, information and knowledge, as well as backups, reside in Brazilian territory. The Ministry of Planning (MPDG) has already released guidelines for its government procurement of cloud computing for public administration, which follow the terms set forth in Complementary Norm 14, and would require that some services should be executed in the national territory, which includes storing the data and information of the contracting party in physically installed datacenters in Brazil.

China: The Chinese government is exerting greater control over where commercial data is stored and how it is transferred. Data localization requirements have appeared in a wide range of Chinese policies, making their impact broadly felt across all sectors of China's economy, including banking, insurance, credit rating, mapping, health care, power generation, and cloud computing. Below is the primary legal framework and authority for data localization:

- Cybersecurity Law (CSL): Effective June 1, 2017, China's CSL sets forth a potentially expansive scope to store personal information and important data—both vaguely defined terms—within China's borders. Article 37 of the law requires all personal information and important data gathered or generated by critical information infrastructure (CII) operators to be stored in China. CII operators can transfer information and data out of China if they have a necessary business requirement and can conduct and pass a security assessment. The definition and scope of CII are essential to assessing the data localization requirement on industry. Article 31 of the CSL gives a broad definition that is both vague and expansive and requires the State Council to formulate a specific CII administrative regulation.

- Regulation on the Protection of Critical Information Infrastructure (CII): Issued for public comment in July 2017, this draft regulation sets forth significant and stringent regulatory obligations, including requirements to store important data and personal information locally and a mandatory review process to move data outside China. Similar to the CSL, the draft regulation provides a broad and unclear scope for CII—including everything from telecommunication networks, broadcasting networks, Internet, and other information networks to organizations that provide cloud computing, big data, and other information services.

- Security Assessment Measures for Exporting Personal Information and Important Data: The measures introduced by the Cyberspace Administration of China (CAC) in April 2017 implement Article 37 of the CSL, outlining security assessment requirements for companies that export data overseas. While the CSL only requires a security assessment for CII operators, these measures significantly expand the scope of cross-border data flow restrictions to all network operators, which could conceivably encompass any company. After significant pushback from industry, CAC granted a 19-month grace period, which will take effect

December 2018, for businesses to comply with the measures, but it does not appear to have addressed industry's substantive concerns.

- Guidelines for Cross-Border Data Transfer Security Assessment: China's National Information Security Standards Technical Committee (TC 260) issued the draft guidelines for public comment in October 2017. The latest draft broadens the definition of "operations within the territory of China" to network operators that are not registered in China but provide products or services inside the country. It also expands the definition of data exports to data that is not transferred to or stored outside of China but is accessed and viewed by overseas individuals or organizations (excluding public information/websites). In combination with China's data localization requirements, the cross-border data flow restrictions are raising costs and creating an uneven playing field. Restrictions on cross-border data transfer are advantageous to domestic companies through easier access to data on one of the two largest national populations as data is regarded as a national strategic resource.

India: In April, the Reserve Bank of India (RBI) published The Notification on Storage of Payment System Data (Data Storage Requirement) mandating payment system operators to store payment system data "only in India" with unfettered access for regulatory purposes and audit reporting requirements. In July, India's Ministry of Finance released the Record of Meeting Minutes in which it acknowledged concerns around the requirement to store data "only in India" and the significant challenges the provisions present to American industry operating in India. A circular clarifying the scope and reach of the Data Storage Requirement has not yet been released, and the requirements for data storage, regulatory access, and reporting remain problematic for industry. The RBI should pursue a full industry consultation focused on international best practices for safeguarding financial transactions, reducing data breaches, and implementing rigorous cybersecurity practices.

Indonesia: The Indonesian government's issuance of Government Regulation No. 82 of 2012 requires U.S. companies to establish both data centers and disaster centers within Indonesia. The requirement to locate data centers and disaster recovery centers in Indonesia that appears in Article 17.2 of GR82 is also repeated in POJK No. 69 of 2016, POJK No. 38 of 2016, MCIT No. 20 of 2016, MCIT Circular Letter No. 3/2016, Circular 17/52/DKSP, PBI 18/40/2016, and PBI 19/8/2017. In particular, it requires Electronic System Operators (ESOs) for public services to place a data center and disaster recovery center in Indonesia for the purpose of safeguarding and upholding justice and state sovereignty towards its citizen's data. While "public services" is not defined in the bill, it is defined elsewhere in Public Services Law (Law No. 25 of 2009). A company considered to be carrying out public services appears to be covered.

Nigeria: In December 2013, the National Information Technology Development Agency (NITDA) issued Guidelines for Nigerian Content Development in Information and Communications Technology (the NITDA Guidelines) applicable across a wide range of ICT products and services in Nigeria, which has come under subsequent

revisions. The Guidelines require that all consumer data collected by companies in Nigeria be stored locally. The guidelines also require all companies operating within the industry to provide a Local Content Plan. For example, companies determined to be Original Equipment Manufacturers (OEMs), are required to maintain at least 50 percent local content by value, assemble all hardware within Nigeria and maintain fully staffed facilities for this purpose, and maintain in-country research and development departments.

Russia: There are several laws limiting the ability of U.S. companies to operate and move data outside of Russian borders. For example, Federal Law 242-FZ requires data collected on Russian citizens to be stored in data centers located in Russia. This requirement has forced both U.S. firms operating in Russia to rewire their operations and U.S. firms providing services from the United States to consider exiting the market or buying server space in Russia to provide the same services at a higher cost.

South Korea: In Korea, there are a number of legislative and regulatory guidelines around cloud computing and data localization that have been only half-implemented and require attention:

- The Cloud Computing Act (CCA): The Ministry of Science, ICT, and Future Planning (MSIP) enacted *The Act on the Development of Cloud Computing and Protection of Use,* commonly referred to as the Cloud Computing Act (CCA), with the intention of developing Korea into a $3.9 billion cloud services market by 2018. Government agencies responsible for setting specific security guidelines for public institutions' use of cloud services have created a patchwork of competing directives and continue to erect barriers to entry that favor local cloud service providers while also creating unnecessary roadblocks for Korean firms that could benefit from such technologies. U.S. industry applauds the legislative intent of the CCA. In practice, however, the law deters U.S. cloud service providers from entering the Korean market. To fulfill the objectives of the CCA, the Korean government should better coordinate among its ministries to establish a transparent, consistent regulatory environment related to cloud services.

- Data Protection Standards for Cloud Computing Services (CCPA): Related to the CCA, the current Data Protection Standards for Cloud Computing Services require data separation and network separation for all public institutions utilizing cloud services. In Korea, this includes financial services, health care, and educational and government institutions. First, the requirement to separate the data from the public cloud requires U.S. companies to create separate intranets for these institutions, which mitigate the efficiencies that cloud computing offers. On the second requirement of network separation, companies are required to build physical servers in Korea, which are prohibitively expensive. The Chamber is encouraging the government to remove the data separation and network separation requirements for public institutions that are currently included in the CCPA

Guidelines. Alternatively, we recommend that the government of Korea reduce the scope of the public institutions covered by the Standard and limit applicability to a narrowly defined set of institutions.

- Regulation on Supervision of Electronic Finance: U.S. cloud service and financial service providers face a unique set of challenges in Korea, due to the physical network separation requirements established under the Regulation on Supervision of Electronic Finance. The Financial Services Commission (FSC) requires the physical network separation of the information processing system of financial companies in its Regulation on Supervision of Electronic Finance. This requirement prevents the introduction of cloud computing services in the financial services sector. In addition, when the cloud service is allowed, it can be introduced only to a "non-critical information processing system," which is vague and makes the introduction of cloud service extremely difficult in this sector. This excessive regulation restricts the use of cloud computing services in the finance industry.

- Regulation on Financial Institutions' Outsourcing of Data Processing Business and IT Facilities: In addition to the FSC's regulation on supervision of electronic finance, they released a revision to the Regulation on Financial Institutions' Outsourcing of Data Processing Business and IT Facilities in June, 2015. Yet, the revisions have not been fully implemented. The revisions sought to eliminate a provision that restricts offshore outsourcing to financial firms' head office, branch, and affiliates to allow outsourcing to a third party including a professional IT company.

- Korean Personal Information Protection Act: Korea's data protection law has numerous restrictions around the movement of data. For example, Korean branches of U.S. reinsurance companies are unable to transfer personal information offshore for data processing or storage due to an inability to gain user consent, and similar restrictions exist for financial services providers.

Turkey: Data localization requirements exist across sectors in Turkey, specifically targeting the banking and electronic communications sectors. Such sectoral restrictions prohibit banks, and payment system and electronic communication operators from procuring data services from cross-border IT vendors that do not have data centers in Turkey. Some examples include:

- Regulation on Internal Systems of Banks: Article 11 of this regulation stipulates that the primary and secondary data systems of banks in Turkey must be maintained within national borders.

- Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector: Article 15 of the regulation

requires communications operators to retain consumer data within Turkey for one year.

- Communique by Capital Markets Board of Turkey: Another sectoral example that underscores concerns regarding broad powers and uncertainty in the policy environment pertains to a communique that was abruptly published in the Official Gazette on January 5, 2018 by the Capital Markets Board of Turkey (SPK in its Turkish acronym). The vaguely drafted communique required publicly traded companies to keep primary and secondary data in Turkey, limiting company access to innovative cloud services. Following rigorous advocacy efforts, SPK issued a clarification on March 8, without fully addressing industry concerns and preserving language to indicate the original communique could be implemented in the future, lacking a clear timeline.

Vietnam: On June 12, the National Assembly of Vietnam passed the Law on Cybersecurity, which enters into force on January 1, 2019.[3] The scope is overly broad, and the law fails to make adequate use of international standards and best practices for cybersecurity and eschews a risk-based approach that has proven effective at enhancing enterprise security and resilience. Instead, it focuses on *ex ant*e inspections of hardware ill-suited to guard against fast-paced threats and a system of audits and penalties.

The law incorporates a range of policy prescriptions outside the domain of cybersecurity, including requirements to store data locally, for foreign companies to establish a local presence, and for telecommunications companies and "cyberspace service providers" to police free speech on the Internet.[4] Vietnam should narrow the timeframe that data must be retained and to limit the amount of information that must be stored in Vietnam. In addition, the government should clarify whether a copy of the data may be locally stored or whether the data must be exclusively stored in Vietnam. Lastly, the government should adopt a narrow scope of content that cyberspace service providers need to remove, such that they are not tasked with 'policing' broad categories of content on the Internet.

It is notable that certain provisions of the law disproportionately affect foreign companies that want to operate in Vietnam, including local presence requirements and the inability to move data across borders, which raises concerns on whether Vietnam is living up to its trade obligations.

Recommendation: The U.S. government should continue to push for movement of data provisions in trade agreements and via multilateral forums such as the G7, G20, OECD, APEC, United Nations, and WTO. NTIA should work with relevant to adopt a whole of government approach that ensures maximum effectiveness for progress around U.S. digital priorities. In particular, U.S. government advocacy should focus on the benefits and necessity of cross-border

[3] Baker McKenzie. *Vietnam National Assembly Passes the Law on Cybersecurity*. June 2018. https://www.lexology.com/library/detail.aspx?g=843a0ed4-5583-434f-8f56-fc206f14c770
[4] Ibid

data flows to a modern digital economy, and how policy priorities can be fulfilled by other regulatory or policy actions that do not require data localization.

Multi-stakeholder Approach and Multilateral Forums: The multi-stakeholder model has proven to be an effective means to ensure a safe and secure Internet. This model should continue to operate in an inclusive and transparent manner that allows stakeholders to engage in and provide their expertise to policymaking.

ICANN and IANA Transition: The Chamber supported the long-planned transition of the IANA functions, along with needed improvements to enhance ICANN accountability. It continues to urge that implementation benchmarks are met. Efforts to unwind the IANA transition risk disrupting the security, stability, and resiliency of the DNS system. The accountability mechanisms established as part of this transition remain viable, but need to be respected by ICANN. NTIA plays a key role in ensuring that ICANN remains committed to fulfilling the obligations it made during the IANA stewardship transition.

The ultimate goal should be to preserve the safe and secure Internet. The Chamber, therefore, does not believe the IANA Transition should be "unwound" or reversed. Doing so would unnecessarily call into question the legitimacy of the multi-stakeholder model of Internet governance.

In terms of specific governmental (GAC) priorities at ICANN, the Chamber appreciates NTIA's continued active engagement within ICANN and its willingness to stand up for U.S. interests there. Such involvement is exemplified by NTIA's advocacy in regard to the interplay of the E.U.'s General Data Protection Regulation (GDPR) and the WHOIS registrant information database, as well as its strong support for the rule of law with regard to the use of geographic names in the DNS.

International Telecommunication Union (ITU): The ITU is a United Nations specialized agency in which governments alone have voting rights. Many of its Member States have shown ambivalence, if not outright hostility, to the participation of non-governmental stakeholders in its procedures. NTIA should propose reforms at the ITU in pursuit of more inclusive, consensus-based decision making, particularly with respect to Internet-related policy matters. Moreover, the ITU continues to try to expand its remit into areas around emerging technology, privacy, and cybersecurity where the necessary expertise on these issues does not exist. Such work should instead be undertaken in transparent, existing multistakeholder forums that have the expertise and mandate to address these issues. The Chamber expressed some of our concerns with the ITU expanding its reach in our comments around the August 2017 Open Consultation on Public Policy Considerations for OTTs.[5]

G7/G20: The G7 and G20 are important venues for shaping the agenda for several of the world's leading governments as they seek to make policy decisions affecting the digital economy, which then directly impact digital trade. In recent

[5] The Chamber's submission to this consultation can be found here.

meetings, the G7 and G20 have placed an emphasis on the digital economy. The United States has worked to ensure G7 and G20 digital communiques carry the right messages on regulation, combating protectionism, and the benefits that productive engagement with the digital economy holds for every nation. However, behind the scenes it has been increasingly difficult to maintain positive statements related to the digital economy as certain members seek to advance alternative agendas. Without more forward planning, we fear that the digital policy discussions in the G7 and G20 may reach a stand still.

Recommendation: The U.S. government should continue to monitor the progress of the multi-stakeholder approach and work with the U.S. business community to ensure it continues to be transparent while advancing U.S. digital priorities. Further, the U.S. government, led by NTIA, should continue to promote the multi-stakeholder model both domestically and internationally, including the Internet Governance Forum, especially in the face of continued calls by some nations to steer internet governance policy discussions into multilateral institutions.

We urge NTIA to play a leading role to ensure that ICANN resolves disagreement with the recommendations raised in the GAC consensus advice from both its San Juan Communique and Panama Communique regarding WHOIS and the EU General Data Protection Regulation (GDPR). The purpose would be to meet ICANN's stated goal of preserving access to registration data currently contained in the WHOIS framework to the greatest extent possible. With the ITU Plenipotentiary taking place this year, the U.S. government should work with industry to determine best approaches to mitigate the ITU's scope-creep into Internet governance issues as well as propose methods for ITU meetings, particularly those that deal with Internet-related policy issues, to be more inclusive of the global multi-stakeholder community.

Finally, the United States should identify and work with G7 and G20 partners across a range of digital policy matters well in advance of future meetings to develop strong common positions on these issues.

Privacy: Prioritizing data protection at the expense of legitimate uses that benefit citizens will forestall innovation. An optimal regulatory model would favor a nuanced approach where regulation is based on the nature and use of the data that enables legitimate business uses of personal data, fosters cross-border data flows, and empowers consumers to make informed choices. Moreover, data protection regulation must be a coherent, streamlined set of rules that establishes clear authorities to minimize complexity.

Rather than looking to create data protection models based on their economic and societal uniqueness, many countries are simply 'copying and pasting' GDPR. Further, the EU has a proactive strategy for engaging with other countries to promote the adoption of this model and is also exporting the GDPR as the 'gold standard of privacy' through its trade agreements. This advocacy is dangerous as the GDPR is an untested policy, and we are likely to see the full impact of the regulation on forestalling innovation for years to come. Moreover, other countries are developing and promoting their own concepts on privacy that are problematic for U.S. industry.

China: China is moving forward with its Internet Sovereignty model. As China develops its privacy and data protection regime, it is critical to engage relevant

stakeholders to ensure interoperability that benefits consumers, industry, and governments alike. The U.S. business community is concerned that China has been hesitant to address privacy protection and enforcement issues through international cooperation. At present, China is not a member of the APEC Cross Border Privacy Rules (CBPRs) system or the cross-border privacy enforcement arrangement, and its data storage and security assessments are incompatible with existing or emerging frameworks. Industry is concerned that China's approach to data protection and privacy—which unreasonably focuses more on where rather than how data are stored in the name of privacy and cybersecurity—will risk fragmenting the Internet along national or regional borders

European Union (EU): The Chamber has a number of concerns with the European Union's approach to privacy.[6]

- GDPR: Industry recognizes that GDPR is law in the European Union and has spent significant time and resources coming into compliance. However, important policy questions around GDPR's implementation remain that will continue to impact American industry. Further, some provisions within GDPR appear at odds with other legitimate policy objectives that the EU should be considering. For example, most small businesses and startups already start at a disadvantage against larger, existing players that have massive amounts of data to utilize. Having to comply with GDPR creates further disadvantages for small businesses as they are unable to access complex legal and compliance guidance easily.

- ePrivacy Regulation: The ePrivacy Regulation currently being discussed in the European Parliament and Council will create further overlap and confusion with GDPR. Continuing to layer sector-specific regulation will only create more uncertainty and cost for companies.

- EU-U.S. Privacy Shield: The Privacy Shield is a vitally important tool for American and European companies to continue to transfer data across the Atlantic and do business, which sets a high standard for the protection of consumer data. The framework has come under scrutiny by the EU's Article 29 Working Party (WP29)[7] and the European Parliament,[8] with both calling for the U.S. government to prioritize the appointment of an Ombudsperson and members of the Privacy and Civil Liberties Oversight Board (PCLOB). The European Parliament's non-binding resolution calls for the European Commission to suspend the framework if concerns are not addressed by September 1. Meanwhile, the WP29 stated that if the concerns are not

[6] Some of the Chamber's top concerns with GDPR are outlined in this blogpost.
[7] Article 29 Data Protection Working Party. *EU-U.S. Privacy Shield – First annual Joint Review.* November 2017. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782
[8] European Parliament. *Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)*. July 2018. http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN

addressed in in the given time frames, European DPAs will take appropriate action, including bringing the Privacy Shield Adequacy decision to national courts and the European Court of Justice.

Kenya: The Kenyan Parliament's Committee on Information, Communication, and Technology recently released the 2018 Data Protection Bill. The legislation is partially based on GDPR but includes broad and vague provisions that would be detrimental to businesses in the market by limiting international transfers, requiring that processing only take place under consent, and enforcing the law through criminal punishment and incarceration.

Turkey: Turkey's Personal Data Protection Law no 6698 was published in the Official Gazette in April 2016 and all articles are now in force. Secondary legislation around the law was prepared by the Personal Data Protection Authority (DPA), which has been established in January 2017. Two pieces of this secondary legislation bring critical liabilities on data controllers such as registering with the Data Controllers' Registry and Periodic Deletion of Personal Data. Further, the DPA has authority to determine the countries with adequate data protection measures where international transfers can occur. A list of countries is expected sometime toward the end of 2018. Overall, the DPA has broad legislative powers and expansive authority on Turkey's data policies. As DPA holds a key role in swaying data localization policies, there is concern among key stakeholders that inadequate consultation with the industry may lead to further uncertainty in the drafting and implementation of critical policies.

Latin America: GDPR-style regulations are emerging across Latin America. For example, Brazil, Chile, Argentina, El Salvador, and Honduras are all currently using the GDPR as a template to create or update their privacy regulations. In May of this year, the Ibero-American Data Protection Network, composed of countries such as Argentina, Chile, Colombia, Mexico, Peru, Uruguay, and others, have embraced new data protection standards fashioned from GDPR.

APEC: The APEC CBPRs have proven to be an important alternative to a GDPR approach that offers privacy protections while still allowing for interoperability between privacy regimes and cross-border data flows. There has been significant progress made over the past couple of years as six APEC economies are now APEC CBPR members. The APEC model should continue to be promoted in APEC and non-APEC countries as it creates interoperability and allows cross-border data flows without diminishing privacy protections.

Multilateral forums: Increasingly, international forums, such as the International Telecommunication Union (ITU), are looking to discuss and act on privacy issues. While some conversations on the issues can be helpful, ITU is not the appropriate forum for any action on privacy in this space. Given that privacy issues cut across a wide range of sectors and industries of all sizes, such action would likely just create more confusion in the international system. Further, the EU is looking to the G7, G20, and OECD as opportunities to push GDPR.

In addition, the International Standards Organization (ISO) has commenced a project to create a standard for privacy by design in consumer goods and services (ISO/PC 317), which would attempt to address privacy "preventatively" at the product and service design phase and prior to commercialization. This important effort would bring value to the global business community by creating a consistent set of guidelines.

Recommendation: NTIA should encourage a whole of government approach to ensure that the U.S. government actively supports international privacy frameworks that facilitate digital trade and the seamless movement of data, pushing back against the contagion of GDPR in other countries and multilateral fora as well as China's push for its own restrictive vision of privacy. The U.S. government should work with partners to promote an approach to privacy in multilateral forums that is focused on interoperability rather than members adopting one entity's approach to privacy. In addition, it should create a strategy around how the momentum with the APEC CBPRs can be continued as well as promote similar approaches in other non-EU countries and regions, such as Latin America. Finally, the E.U.-U.S. Privacy Shield should be maintained. We applaud the Administration for its efforts last year that ensured the Privacy Shield successfully made it through its first annual review and look forward to supporting the review this year post Europe's GDPR implementation.

Security: The Chamber generally believes that cybersecurity needs to be rooted in global, industry-driven, and voluntary standards and practices. Efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment. In a global economy, ill-conceived and government-directed security-related rules erect trade barriers along national boundaries that may, in practice, burden industry while failing to achieve legitimate policy objectives. They may also limit competition and the economic benefits of participating in a robust, global ICT industry, without providing security benefits and potentially weakening security. Such approaches burden multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

The Chamber shares NTIA's belief that cybersecurity risks should not be viewed exclusively as a national security threat but as a threat to economic growth and innovation. We appreciate the sensitive national security concerns and equities often at play in multilateral cybersecurity discussions. We urge NTIA, however, to prioritize building public-private consensus around policies that advance system resiliency against cyber threats and trust in systems, which will ultimately stimulate economic growth and innovation. We advocate for smart cybersecurity legislation, regulation, and policies that build and sustain relationships between industry and government in order to quickly counter fast-paced cyber threats.

Aligning enterprise security measures requirements: The Chamber supports alignment of security requirements with the U.S. National Institute of Standards and Technology (NIST) cybersecurity framework or the International Organization for Standardization (ISO) Information Technology—Security Techniques—Cybersecurity and ISO and IEC Standards (ISO 27103). U.S. and foreign governments' cyber policies and laws should be aligned with the approach underpinning the Framework for Improving Critical Infrastructure Cybersecurity. Industry is enthusiastic about the

framework because it is neither biased toward any given country's laws nor bound by outdated and inflexible rules and procedures.

A number of governments have embraced the framework, including Italy,[9] Ireland,[10] Israel, Japan,[11] Malaysia, and Uruguay.[12] The Chamber is advocating for governments to align security requirements for critical infrastructure to the framework. It was constructive that the Network and Information Systems (NIS) Cooperation Group encouraged European Members States to use international standards (e.g., ISO 27000) as a means of complying with the NIS Directives Article 14 (i.e., security measures) requirements.[13]

Risk-based Approaches: Cyber regulatory philosophies need to be risk-based and performance-based. Risk management is a foundational principle for information security. The Chamber supports performance standards that specify the outcome required but *leave the specific measures or techniques to achieve that outcome up to the discretion of the regulated entity* in partnership with government entities. The Chamber opposes attempts by governments to mandate *preferred cybersecurity solutions*—whether a practice (e.g., labeling), a process (e.g., certification), or an IT product or service—without the consent of affected owners and operators. Top-down approaches to instituting information security measures and controls should not have a place in a genuinely collaborative program.

Aligning or harmonizing existing regulations: Policymakers should seek to harmonize existing cybersecurity regulations and mandates with tools such as the framework, so that businesses can stay agile and responsive to attempted incursions. The Chamber especially welcomes government entities forming partnerships with industry to enhance the security and resilience of critical infrastructure.

Protecting, not forcing, information sharing: The United States and its allies should enhance the situational awareness of organizations through protected rather than mandatory, information sharing. Proactive cyber threat data sharing informs organizations of potential threats (e.g., malicious code, indicators of compromise, tactics, techniques, and procedures) so that they can protect and defend their networks. Threat data sharing frameworks should include the following parameters when sharing information with industry peers or government partners: multidirectional sharing (e.g.,

---

[9] Government of Italy. CIS-Sapienza and National Cyber Security Laboratory. *A National Cybersecurity Framework*. http://cybersecurityframework.it/en

[10] Government of Ireland. Department of Communications, Climate Action and Environment. *Network and Information Systems Directive*. https://dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/eu-developments/cyber-security-legislation-/Pages/Cyber-Security-Legislation.aspx

[11] Government of Japan. Information-technology Promotion Agency, English Translation of the NIST framework (February 2014), https://www.ipa.go.jp/files/000038957.pdf

[12] Government of Uruguay. Agency for Electronic Government and the Information and Knowledge Society, *Cybersecurity framework v4.0* (June 2018), https://agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad.html

[13] NIS Cooperation Group. *Reference document on security measures for Operators of Essential Services*. February 2018. http://ec.europa.eu/information_society/newsroom/image/document/2018-24/reference_document_security_measures_oes_1B549F1B-9144-40B4-AFC2A5441E087584_52944.pdf

government to industry, industry to industry); voluntary sharing of information; and safe harbor provisions, including liability under data protection and antitrust laws. Threat information sharing must protect privacy. Information sharing arrangements are most successful when they build on trust, enable bidirectional sharing, and enable victims of attacks to share information about both successful intrusions and near-miss attempts without fear of being investigated, sued, or held criminally liable.

In contrast, forced reporting is likely to create substantial noise in the system and lead to a diffusion of businesses' limited resources toward compliance and away from risk management activities. Instead of assigning blame to organizations when they come forward to report a breach, laws and policies should facilitate continuous and candid collaboration between industries and agencies outside of the enforcement space.

The Chamber believes that legal protections offer an incentive and remove barriers to non-federal entities to share cyber threat data in real time, at machine speeds, with industry peers and government partners for cybersecurity purposes. Legal safe harbors on their own may not serve as incentives for non-federal entities to share and, therefore, it is important for government sharing programs to create a clear benefit for entities to participate.

The Chamber recognizes the self-regulatory model embodied by the U.S. framework is not the only model used by foreign governments. Singapore's recently enacted Cybersecurity Law envisions an information-sharing ecosystem built on a closer regulator and regulated entity relationship.[14] The Financial Services Information Sharing and Analysis Center, and the Monetary Authority of Singapore, opened the Asia Pacific Regional Analysis Centre in 2017. The centre is meant to manage, analyze, and share actionable threat information in real time across nine Asia Pacific countries.[15] Similarly, the United Kingdom's Cyber Security Information Sharing Partnership (CiSP) operated by the National Cyber Security Centre (NCSC), is a joint industry and government initiative set up to exchange cyber threat information in real time and in a secure, confidential, and dynamic environment while increasing situational awareness and reducing the impact on businesses. As of December 2017, over 4,020 organizations and 9,097 individuals have signed up to use CiSP.[16] These industry-supported alternatives to regulated and mandatory information-sharing frameworks offer good examples of where NTIA can advance industry's information sharing policy priorities internationally.

Reporting cyber incidents in productive ways: The Chamber supports the alignment of cyber incident and data breach reporting requirements across multiple jurisdictions. Preventing significant cyber incidents from interrupting or disrupting the continuity of critical infrastructure services and protecting individuals' sensitive personal information from theft or illicit uses are top industry priorities. Technology-neutral and flexible legislation would help businesses by reducing the complexity around complying with reporting requirements across multiple government jurisdictions. The Chamber

[14] Government of Singapore. *Cybersecurity Act of 2018*. https://csa.gov.sg/legislation/cybersecurity-act
[15] FS-ISAC. *FS-ISAC and MAS to Strengthen Cyber Information Sharing Across Nine Countries* (November 2017). https://fsisac.com/article/fs-isac-and-mas-strengthen-cyber-information-sharing-across-nine-countries
[16] NCSC. *Cyber Security Information Sharing Partnership* (Accessed July 2018). https://ncsc.gov.uk/cisp

urges policymakers to be mindful that both consumers and businesses are victims of cybercrimes. Consumers should be notified in a reasonable and timely manner after a reportable incident or data breach. However, rather than specifying a specific time frame, the Chamber recommends reporting frameworks that permit maximum flexibility. Qualifiers, where feasible, are critical to fostering good investigations and quality, accurate, and timely reporting.

One of the cornerstones of most primary cybersecurity laws introduced in legislative bodies is the requirement that regulated entities must report cyber incidents, sometimes with qualifiers (e.g., significant, serious, or harm to national security and public safety), to government entities. An example is the European Union's Network and Information Systems Directive,[17] which seeks to achieve a high level of network and information systems security for operators of essential services and digital service providers by requiring that member states pass national laws containing, among other things, mandatory incident reporting requirements.

As a result, a patchwork of duplicative, overlapping, and burdensome mandatory reporting requirements now exist in the European Union. For example, if an Italian-based financial services firm, designated as an operator of essential services, is the victim of a data breach resulting from a cyber incident, under current European laws, that firm must report to a competent authority, a data protection authority, a sector regulatory, the European Central Bank, and the European Banking Authority. The Chamber acknowledges that mandatory incident reporting may be required in certain circumstances, such as national security and public safety, but we believe that government entities are responsible for clearly defining a need and outcome for how data is used and that reporting should be narrowly defined. Future policy efforts should focus on the alignment of reporting requirements

Building international norms: Governments should continue to take steps to promote the stability of the open, interoperable, and global Internet and to reduce the potential for state conflict to undermine this stability.

Recommendation: The Chamber recommends that NTIA work with its U.S. government partners to promote alignment of cybersecurity requirements to industry-supported tools, like the framework and international standards. Bias toward national approaches to cybersecurity (e.g., China, Vietnam) weakens risk management activities and the promulgation of outdated and inflexible rules, procedures, and technologies divert scarce information security budgets to costly compliance mandates. The Chambers believe that cybersecurity governance is at an inflection point and seeks government partners to advocate for voluntary, flexible, and technology neutral regulations that benefit public and private sectors alike.

Emerging Technologies and Trends: Emerging technologies are creating new interdependencies between developers, providers, and users. In fact, 68 percent of American

[17] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). http://bit.ly/2a6gFgw

voters say technology will make their communities operate better.[18] 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), for example, 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 20.4 billion connected devices by 2020, over 30 times the number in 2009.[19] Employing one-size-fits-all standards for connected devices is not the right match to confront face-paced commercial demands and risks that companies face online. Countries, from Brazil to Malaysia, are increasingly creating IoT strategies that endeavor to create an environment for investment and growth. While research and development are key components of such strategies, regulation is too.

Artificial intelligence (AI) and automated decision-making are also increasingly coming under the scrutiny of regulators. Many of these concerns currently focus on the potential for these technologies to exacerbate bias. In response, regulators are articulating a desire to make algorithmic decision-making more transparent by forcing companies to explain their decisions or turn them over. Algorithms should be treated as intellectual property in the same way that source code is. AI will be the catalyst of major developments across sectors enhancing economic growth and better our societies. AI is still nascent, and it would be a mistake to attempt to address the issue with broad, overarching regulation. Therefore, a more risk-based and flexible policy framework that focuses on accountability would enable AI to flourish.

Many countries, as well as the International Telecommunication Union (ITU), are also looking to push further burdensome and outdated regulations on over-the top (OTT) services and applications. When a foreign government indicates its intent to regulate OTTs, it is 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 key drivers of growth in the global economy including texting, sharing of user-generated video content, cloud and IoT services, money transfers, and mobile payments. The proposed regulations in countries such as Indonesia and Vietnam would 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.

A disturbing trend, and one that NTIA should work with domestic and international partners to address, is the rapid global growth of "streaming piracy" using piracy devices and

[18] U.S. Chamber of Commerce Technology Engagement Center (C_TEC) http://ctecintelligence.com/
[19] Liam Tung, "IoT devices will outnumber the population this year for the first time," ZDNet. Feb. 7, 2017. available at https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-firsttime/.

apps.[20] There has been a growing level of activity, and international cooperation, among governments and enforcement agencies to put the providers of pirate devices and apps out of business, but the levels of activity are not yet commensurate with the enormous threat that piracy devices and apps represent to both rights holders and legitimate distributors. Laws and enforcement policies to stop piracy are being implemented globally in a manner that is fully consistent with free expression and the desirability of continued technological innovation.

Recommendation: Emerging technology is being increasingly discussed in forums such as the G20, ITU, and OECD. While discussions are helpful, given the nascent stage of these technologies, it is critical that multilateral organizations do not undertake the creation of guidelines or regulations. The U.S. government should work with foreign policymakers and regulators to educate them on creating an environment that enables innovation and investment to ensure users are able to benefit from increased use of emerging technologies, while also cooperating to reduce abuses such as IP theft. Unnecessary and unproven regulation only serves to stifle innovation and investment, dampen competition, and harm consumers. Instead, the focus should be on facilitating a discussion based on evidence and stakeholder expertise.

***

The Chamber appreciates the opportunity to offer its views to the NTIA on its international Internet policy priorities. At a time when governments are developing either flexible plans or top-down directives, NTIA's positive role in international Internet policy settings is significant to America's engagement strategy and U.S. business interests at home and abroad.

Sincerely,

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

[20] "Piracy devices and apps" refers to the fast-growing international phenomenon of set-top boxes and other devices that are configured to enable easy access over the into the piracy ecosystem to watch live and on-demand content.