SIIA Accelerating Innovation in Technology, Data & Media
202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

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

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit the following comments in response to the National Telecommunications and Information Administration's Notice of Inquiry published in the Federal Register on June 5, 2018. SIIA's suggested priorities for NTIA international engagement follow in this paragraph and more detailed information is provided below and is keyed to NTIA questions.

1) Cross-border data flow commitments, especially through trade agreements.
2) Cross-border data flow interoperability mechanisms between different privacy systems, including risk-based systems such as the U.S. regime, e.g. Asia Pacific Economic Cooperation Cross Border Privacy Rules.
3) Continued collection of and access to WHOIS information.
4) Privacy dialogues should distinguish between B2B and B2C obligations.
5) Pursue common approach to Artificial Intelligence, blockchain and other emerging technologies.
6) Oppose extra-territorial application of other countries' privacy laws, for instance the right to be forgotten.
7) Pursue law enforcement sharing treaties per the CLOUD Act.
8) Support streamlining of Mutual Legal Assistance Treaty (MLAT) processes.
9) Prioritize access to broadband at upcoming ITU Plenipotentiary.
10) Send high-level Administration official to Internet Governance Forum (IGF).

I. The Free Flow of Information and Jurisdiction

A. What are the challenges to the free flow of information online?

With respect to the economic dimension of challenges to information flows (digital trade and cross-border data flows), see SIIA's March 6, 2018 testimony [1] before the U.S. International Trade Commission. The challenges usually manifest themselves through data localization requirements. For an estimate of the costs of the data localization, see this European Center for International Political Economy (ECIPE),

[1] Prepared Testimony of Carl Schonander Senior Director for International Public Policy Software & Information Industry Association Before the United States International Trade Commission On Investigation No. 332-562 Global Digital Trade 2: The Business-to-Business Market, Key ForeignTrade Restrictions, and U.S. Competitiveness Investigation No. 332-563
Global Digital Trade 3: The Business-to-Consumer Market, Key Foreign Trade Restrictions, and U.S. Competitiveness March 6, 2018

report.[2] The 2018 U.S. Government National Trade Estimate report,[3] especially the section on digital trade, describes the challenges well. Among the key barriers to digital trade, SIIA considers China's restrictions on cross-border data flows and data localization requirements; restrictions on leased lines on VPNs; cloud computing restrictions; and, China's web filtering and blocking to be the most significant globally. This Information Technology & Innovation Foundation (ITIF) report [4] is another excellent source of information on digital trade barriers and their costs.

Regarding limitations on the free flow of information online motivated by political reasons (Internet censorship, for instance), the U.S. government's annual human rights reports contain relevant information. The Freedom House reports on Freedom on the Net are also an excellent source of information. Not surprisingly, China is considered the least free from an Internet Freedom standpoint. But, it is worthwhile noting that there is a group of countries, often close to the United States, somewhat in the middle with respect to Internet Freedom according to Freedom House. This group includes Brazil, Colombia, Mexico, India, and Singapore. It might be worthwhile prioritizing U.S. diplomatic engagement on Internet Freedom matters with these countries as they may be more willing to engage in a dialogue on these issues than, say, China, which is at the bottom of the table on Internet Freedom according to Freedom House.

B. Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S. companies and users in general?

See answers to A.

C. Have courts in other countries issued internet-related judgments that apply national laws to the global internet? What have been the practical effects on U.S. companies of such judgements? What have the effects been on users?

In March 2016, the French Data Protection Authority (CNIL) fined Google Euros 100,000 for not delisting search results globally, not just from EU domains, if the search result had to be delisted per an approved right-to-be-forgotten request. SIIA commented in this April 16, 2016 blog[5] that globalizing the right-to-be-forgotten sets a dangerous precedent because it could legitimize measures by non-democratic regimes to impose censorship beyond their borders. SIIA urged European courts to reject this approach. In July 2017, the French Conseil d'Etat court referred the case to the European Court of Justice (ECJ) for adjudication. The practical effect of the right to be forgotten for companies is the compliance cost and for users a less informative Internet. For SIIA, a key goal is for the right to be forgotten not to be applied extraterritorially. Should the ECJ side with CNIL on this matter, SIIA urges the U.S. government to advocate before the European Commission and Member States for a legislative amendment to the General Data Protection Regulation that would clarify that it does not apply extraterritorially.

D. What are the challenges to freedom of expression online?

See answers in A.

---

[2] "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper No. 3/2014
[3] National Trade Estimate, 2018
[4] Information Technology & Innovation Foundation (ITIF), "Cross-Border Data Flows: Where are the Barriers, and What do they Cost?", Nigel Corey, May 2017
[5] CIO, "Globalizing the right be forgotten sets a dangerous precedent," Mark MacCarthy, April 6, 2016

E. What should be the role of all stakeholders globally—governments, companies, technical experts, civil society and end users—in ensuring free expression online?

International conventions on freedom of expression should apply online as well as offline. The Universal Declaration of Human Rights Article 19 remains valid today: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This should be the baseline all stakeholders apply. That said, even democratic nations with a demonstrated commitment to free speech have different rules on hate speech, political advertising/advocacy, libelous speech, extremism, intellectual property protection, pornography, and other issues. These are complicated political, technical, and legal issues. Sometimes countries will legislate in this area and that is not an a priori illegitimate option. However, SIIA's preferred solution is for stakeholder developed voluntary schemes. The May 31, 2016 EU "Code of Conduct on Illegal Online Hate Speech" is an example of such a mechanism. Stakeholders should engage in good faith with respect to addressing these issues. Broadly speaking, companies have three fundamental responsibilities [6] with respect to, for instance, online extremism, and these responsibilities can be extrapolated to work in other policy settings as well. Companies have takedown responsibilities; countervailing responsibilities to foster free speech and association; and, they have an affirmative responsibility to take steps to counter violent extremism. These are not legal requirements in U.S. law. Ideally, they should not be legal requirements elsewhere. However, if countries do legislate, NTIA should monitor and when necessary advocate for a framework which preserves freedom of expression, addresses negative online phenomena, and, at the same time, allows for continued innovation.

Democracies such as the United States need to ensure that elections are as free as possible from election interference. This is why the reported May 23, 2018 meeting [7] between eight tech companies and U.S. intelligence officials was important. Stakeholders in democratic nations should work together to ensure that elections are as free as possible from outside interference.

F. What role can NTIA play in helping to reduce restrictions on the free flow of information over the internet and ensuring free expression online?

NTIA should work with the relevant interagency partners within the U.S. government to develop an integrated U.S. government strategy to promote the free flow of information over the internet and free expression. That strategy should combine all the relevant elements of national power, including diplomatic, technical, military, intelligence, and economic (especially) trade assets.

G. In which international organizations or venues might NTIA most effectively advocate for the free flow of information and freedom of expression? What specific actions should NTIA and the U.S. Government take?

With respect to the free flow of information (essentially cross-border data flows), the most effective tool is a high-quality trade agreement. This is why SIIA strongly supports the Administration's updated digital

[6] SIIA Digital Discourse Blog, "What are the Responsibilities of Tech Companies in an Age of International Terrorism?", Mark MacCarthy, March 24, 2016
[7] The New York Times, "Top Tech Companies Met with Intelligence Officials to Discuss Midterms," Sheera Frenkel and Matthew Rosenberg, June 25, 2018

negotiating objectives for the NAFTA.[8] These goals should be applied to other trade agreements as well. The Administration should promote high-quality empirical work on the value of cross-border data flows.

Freedom of expression is a human rights issue. The United States should engage in all available fora to pursue freedom of expression online. Should the Trump Administration decide to reengage with the United Nations Human Rights Council, it should prioritize diplomatic engagement to deepen the Council's commitment to freedom of expression online.

H. How might NTIA better assist with jurisdictional challenges on the internet?

NTIA should advocate within the interagency for using the recently approved Clarifying Lawful Use of Data (CLOUD) Act to facilitate access to data of interest to law enforcement agencies from U.S. friends and allies such as the European Union and other countries. SIIA takes no position on whether the U.S. government should conclude a law enforcement sharing agreements with the EU or individual Member States, but NTIA should advocate within the interagency for concluding as many agreements as possible as soon as possible. And although the CLOUD Act may relieve immediate pressure to reform the Mutual Legal Assistance Treaty (MLAT) process, it remains important to streamline the MLAT process. Again, NTIA should advocate for this within the interagency.

II. Multistakeholder Approach to Internet Governance

A. Does the multistakeholder approach continue to support an environment for the internet to grow and thrive? If so, why? If not, why not?

The multistakeholder approach is a necessary but not sufficient condition for the internet to continue to grow and thrive. With respect to the internet governance functions overseen by ICANN, the multistakeholder approach has proved valuable, albeit sometimes slow. For example, the work associated with developing a new collection and access model for WHOIS data could arguably be completed more quickly. However, it is not likely that this issue could be resolved satisfactorily more expeditiously if the substance of ICANN's management of the internet were to be managed in a multilateral, as opposed to multistakeholder, setting.

With respect to the Internet writ large, it would be preferable to avoid balkanized or regional Intranets along the lines of China's "Great Wall." In order to avoid this outcome, NTIA should continue to encourage interoperability mechanisms such as the APEC Cross Border Privacy Rules system. Such mechanisms should be recognized and legitimized in 21st century trade agreements that establish cross-border data flows as the default.

B. Are there public policy areas in which the multistakeholder approach works best? If yes, what are those areas and why? Are there areas in which the multistakeholder approach does not work effectively? If there are, what are those areas and why?

More technical subjects tend to lend themselves to multistakeholder approaches. The work conducted by the Internet Engineering Task Force (IETF) is a good example. The development of the Domain Name System Security Extensions (DNSSEC) is an important IETF success story, which is enhancing trust in the internet thanks to great security afforded by DNSSEC. Even issues where players have different political

[8] USTR, "Summary of Objectives for the NAFTA Renegotiation," November 2017

and/or commercial interests can by resolved through the multistakeholder process. This is true, for instance, in the access to WHOIS data matter. There is a balance to be struck though, albeit a difficult one for NTIA and the U.S. government to navigate. ICANN policy development processes cannot be permitted to continue for too long or indefinitely when vital U.S. commercial interests are at stake.

C. Are the existing accountability structures within multistakeholder internet governance sufficient? If not, why not? What improvements can be made?

D. Should the IANA Stewardship Transition be unwound? If yes, why and how? If not, why not?

SIIA is not aware of any available mechanism that would allow the IANA Stewardship Transition to be unwound.

E. What should be NTIA's priorities within ICANN and the GAC?

Ensuring continued access to and collection of WHOIS data.

F. Are there any other DNS related activities NTIA should pursue? If yes, please describe.

G. Are there barriers to engagement at the IGF? If so, how can we lower these barriers?

Barriers to IGF engagement are minimal. The IGF remains a valuable forum and NTIA should continue to engage with IGF USA and the global IGF.

H. Are there improvements that can be made to the IGF's structure, organization, planning processes, or intercessional work programs? If so, what are they?

Improvements are always possible. However, the value of IGF is precisely that it is somewhat informal and that it does not produce outcome documents. The somewhat informal nature of the IGF should be maintained.

I. What, if any, action can NTIA take to help raise awareness about the IGF and foster stakeholder engagement?

The Washington, D.C. government relations community is aware of IGF so NTIA probably does not need to do more outreach to Washington, D.C.-based actors. However, it might be worthwhile for NTIA to intensify IGF information dissemination at regional events featuring Commerce Department officials.

J. What role should multilateral organizations play in Internet governance?

None with respect to the tasks assigned to ICANN. This the redline that NTIA should maintain. SIIA encourages NTIA to continue to play a leadership role within ICANN's Governmental Advisory Committee (GAC). Although the GAC operates by consensus, the U.S. government has proved effective in the past in using this venue to influence ICANN.

With respect to other multilateral organizations, "Internet governance" means different things to different people. It is a broad concept with many different facets. It is not diplomatically possible to prevent multilateral organizations from discussing Internet governance in the broadest senses. The

challenge for the U.S. government is to attempt to steer multilateral organizations into focusing on their core mission(s) in a way that is positive for the future of the internet. For instance, the ITU should be encouraged to work on policies that enhance access to broadband. The WTO's E-Commerce committee should be encouraged to promote frameworks permitting cross-border data flows. The APEC work on Cross Border Privacy Rules should continue. The United States should promote a freedom of expression agenda aggressively in appropriate UN fora. The OECD Internet Policymaking Principles are a successful example of how the United States succeeded in steering an international organization into producing a good outcome, in this case on a topic that is, in fact, directly applicable to Internet governance. NTIA should continue to make OECD engagement a priority.

III. Privacy and Security

A. In what ways are cybersecurity threats harming international commerce? In what ways are the responses to those threats harming international commerce?

To the extent there are breaches in cybersecurity, trust in the Internet is undermined, which impedes its use for commercial purposes. However, it is difficult, if not impossible, to estimate what the quantitative effects might be. The Administration correctly identified Chinese cyber-enabled theft of intellectual property as a major problem in its March 22, 2018 report entitled: "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974." [9] SIIA has joined other trade associations in letters to the Administration and the Congress agreeing that there are major trade policy problems with China that need to be addressed, but that tariffs are not an appropriate response. Instead, SIIA advocates working with U.S. allies to create an international coalition to address problems stemming from China.

B. Which international venues are the most appropriate to address questions of digital privacy? What privacy issues should NTIA prioritize in those international venues?

The OECD has a productive record of addressing questions of digital privacy. The 2013 OECD Privacy Guidelines are a good basis for continued discussion. The OECD notes that two themes run through these updated guidelines: a focus on risk management and the need to address the global dimension of privacy through improved interoperability. SIIA supports these themes. There should also be a recognition that B2B companies and B2C companies have different privacy challenges, which should be reflected in laws and regulations. And most fundamentally, NTIA should advocate for the idea that as long as privacy regimes address identified risks to consumers and companies, those regimes to do not have to be identical. This is why the TransPacific Partnership's (TPP) Article 14.8 Footnote 6 was so important. The footnote made clear that a signatory to the TPP could comply with the affirmative obligation to have a privacy system through a U.S.-style sectoral privacy system. This goal is all the more critical at this time as many countries find the EU General Data Protection Regulation (GDPR) law a convenient system to emulate. It will take considerable political will and diplomatic work to push back against this trend.

[9] Office of the United States Trade Representative, Executive Office of the President "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," March 22, 2018

IV. Emerging Technologies and Trends

A.What emerging technologies and trends should be the focus of international policy discussions? Please provide specific examples.

Issues surrounding Artificial Intelligence (AI) will be an important focus of international policy discussions in the coming years. The June 13, 2018 Charlevoix Common Vision for the Future of Artificial Intelligence is a good point of departure for how the United States should handle AI discussions in international fora, especially point 12, which calls on signatories to: "Support an open and fair market environment including the free flow of information, while respecting applicable frameworks for privacy and data protection for AI innovation by addressing discriminatory trade practices, such as forced technology transfer, unjustified data localization requirements and source code disclosure, and recognizing the need for effective protection and enforcement of intellectual property rights." NTIA should oppose AI regulations but work with other countries on principles as appropriate. The EU will be releasing principles at the end of 2018. There may be an opportunity for NTIA to engage in a discussion with the EU on the principles while they are still in draft.

B. In which international venues should conversations about emerging technology and trends take place? Which international venues are the most effective? Which are the least effective?

The OECD is a potentially effective venue. It does take a considerable investment in resources though to get to good outcomes even though most of the OECD's members are at a similar level of development as the United States. The March 27-28, 2018 OECD report entitled "Transformative Technologies and Jobs for the Future" [10] is indicative of a constructive approach to emerging technologies such as AI, which NTIA can work with. NTIA should encourage the OECD to continue to measure the impact of the importance of data, something that the OECD says is needed in the report.

C. What are the current best practices for promoting innovation and investment for emerging technologies? Are these best practices universal, or are they dependent upon a country's level of economic development? How should NTIA promote these best practices?

The United States has a good framework for promoting innovation and investment for emerging technologies. The EU notes, for instance, in its April 24, 2018 Communication on Artificial Intelligence that in 2016, private AI investment in North America was EUR 12.1 to 18.6 billion; in Asia it was EUR 6.5 to 9.7 billion; and, in Europe it was EUR 2.4 to 3.2 billion. But Asia, especially China, is rapidly catching up. And the United States will not likely match public Chinese investment in AI and other emerging technologies. Nonetheless, the Trump Administration's commitment to a 2% increase in Federal R&D spending is welcome and many of the Administration's actions as described in the OSTP document entitled "Science & Technology Highlights in the First Year of the Trump Administration" [11] are also welcome. In this context, it is critical that as the Administration and the Congress consider new approaches to privacy, that U.S. industry continues to have access to plentiful high-quality data, including personal data, in order to develop cutting edge products and services that stem from emerging technologies. Fundamentally, emerging technologies such as autonomous vehicles and drones depend on highly developed data

[10] OECD, "Transformative Technologies and Jobs for the Future: Background report for the Canadian G7 Innovation Ministers's Meeting 27-28 March 2018

[11] OSTP, "Science & Technology Highlights in the First Year of the Trump Administration," March 2018

analytics techniques. Ensuring that the United States remains the leader in data analytics is the key to continued U.S. leadership in emerging technologies. This SIIA White Paper entitled "Data-Driven Innovation A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data"[12] includes policy recommendations NTIA may find useful in developing policy in this space. Although the recommendations are directed to U.S. policymakers, most if not all of them, can be applied internationally. They are:

1. To meet its full potential, DDI requires a policy framework that provides for an evolving view of privacy rights based on risk and societal benefits.
2. The principle of data minimization should be re-interpreted in light of DDI.
3. Policymakers should encourage de-identification as a way to balance the needs of DDI and privacy protection.
4. Uniform rules should not apply broadly to the collection of personal information and the role of consent.
5. Policymakers should promote technology neutrality and avoid technology mandates.
6. Open standards are critical enablers of DDI, but they must continue to evolve through industry-led standards development organizations, not governments.
7. Policies should allow data collectors and controllers to work with data management and analytics suppliers to comply with privacy and security rules through contracts across varying jurisdictions.
8. Policies must continue to balance the need of protecting the privacy of students, while enabling DDI to greatly enhance the teaching and learning experience.
9. Governments should adopt policies that leverage DDI to make government more efficient and effective and reduce government waste.
10. Governments should continue to embrace open data policies and public private partnerships that maximize access to critical public data.

Once again, SIIA appreciates the opportunity to comment. The United States is a leader in the technologies that NTIA supports. Therefore, NTIA leadership in international internet policy dialogues remains essential. SIIA stands ready to assist NTIA in its mission and is open to providing additional information and/or support upon request.

Sincerely,

Carl Schonander
Senior Director, International Public Policy
Software & Information Industry Association (SIIA)
1090 Vermont Avenue, NW
Washington, D.C. 20005

[12] SIIA White Paper, "Data-Driven Innovation A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data," Public Policy, 2013