UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

November 8, 2018

Mr. Travis Hall
Telecommunications Policy Analyst
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC 20230

RE: NTIA Request for Public Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

Dear Mr. Hall:

The U.S. Council for International Business (USCIB) is pleased to respond to this request for public comments concerning "Developing the Administration's Approach to Consumer Privacy." USCIB is a trade association composed of more than 300 multinational companies, law firms, and business associations, which includes a broad cross-section of the leading global companies in the information and communications technology (ICT) sector. USCIB members welcome this opportunity to offer a cross-sectoral perspective on the challenges of developing a privacy framework in the digital age.

Data Flows, Trust – and Fragmentation

USCIB embraces the view that the free flow of data and information is critical for economic development and growth. According to one study, during the 2005-2014 period, data flows increased by 45 times, and now account for a larger share than global trade in goods. Importantly, the increase in GDP from data flows was an estimated $2.8 trillion. This same study found that some 900 million people have international connections on social media, and 360 million take part in cross-border e-commerce.[1]

Business realizes, however, that the benefits of technology innovation enabled by data flows will only be realized and embraced by consumers, businesses, and governments who trust the online environment and feel confident that the privacy of their personal data will be respected. USCIB members are committed to complying with applicable privacy regulations and recognize their responsibility to adopt recognized best practices to ensure that personal data and information is appropriately secured as technology and services evolve.

As you note, however, the evolution of the digital economy has increased the volume of personal data collected, used, and stored and precipitated a flurry of responses in the global community as well as at the U.S. state level about how to address related privacy concerns. Countries such as China, India, Malaysia, Panama and South Korea have proposed restrictive data protection laws that could significantly harm U.S. companies while also undermining efforts to enhance global

[1] McKinsey Global Institute (March 2016): *Digital Globalization; The New Era of Global Flows*.

interoperability. These approaches range from quite onerous data localization requirements to national privacy frameworks that are administratively burdensome and complex, all of which end up imposing economic costs on the country by undermining their attractiveness as destinations for jobs-creating investment and innovation. They also create an increasingly fragmented regulatory landscape, which imposes added compliance costs on business that hampers continued innovation.

The Government of India, in particular, has proposed a Personal Data Protection Bill that would establish an alarming global precedent and could significantly impede the growth of innovation, investment, entrepreneurship, and industrial growth through strict data localization requirements, restrictions on the cross-border data flows, and extraterritorial application. It is vital that the U.S. continue to exercise global leadership in pushing back against this type of protective approach to personal data protection.

Global Interoperability and Potential "Model" Frameworks

USCIB members comprise global leaders in the ICT sector whose commercial operations span the world. They look to USCIB to leverage access to various global forums enabled by our international affiliations to promote their views on key policy and regulatory issues, privacy being one of them. Consistent with the global reach of our members' operations and USCIB's core competencies, we therefore will focus these comments primarily on the administration's "High-Level Goal" to develop mechanisms that realize greater interoperability among international privacy regimes.

We applaud NTIA for recognizing the need to bridge regulatory differences so there is less fragmentation, data flows seamlessly, and the digital economy continues to evolve. In pursuing development of an interoperable approach, however, it is imperative that we realize an appropriate balance so that privacy frameworks promote consumer/user trust in data-driven technologies while at the same time enabling companies and organizations to use and transfer data in innovative ways that benefit society.

The following frameworks were developed to ensure this balance. In our view, they would serve as models for a globally interoperable framework:

- *OECD's 2013 Privacy Framework* -- USCIB believes that the OECD's 2013 Privacy Framework[2] serves as a solid foundation for an over-arching privacy and data protection framework appropriate for privacy in a digital age. The fact that the 32 OECD member countries endorsed the framework constitutes a strong and broad base of consensus upon which to build the bridging mechanism. We note that the OECD's 2011 Principles for Internet Policy Making[3], which continue to serve as the basis for building consensus on Internet-related policy issues, expressed the general objective of OECD members to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the OECD Privacy Framework.

  Under the aegis of Business at OECD (BIAC), USCIB actively contributed input that shaped the 2013 guidelines. Importantly, the OECD framework principles include many of the NTIA's proposed "Privacy Outcomes," such as:

[2] Organization for Economic Cooperation and Development (OECD), *OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

[3] *OECD Principles for Internet Policy Making* (2011) -- http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf

- The principle that privacy management programs develop appropriate safeguards that are based on privacy risk assessment;
- The principle that personal data should be relevant to the purposes for which they are to be used, i.e., "reasonable minimization;"
- The principle requiring the purposes for which personal data are collected be specified, accompanied by a general policy of openness about developments, practices, and policies, with respect to personal data, i.e., "transparency;"
- The principle that personal data should not be disclosed, made available, or otherwise used for purposes other than those specified without the consent of the data subject. In addition, individuals have the right to confirm whether a data controller has data relating to them and to challenge data relating to them for correction or erasure, i.e., "user control, access and correction;"
- The principle that personal data should be protected by reasonable security safeguards, i.e., "security;" and
- A requirement that the data controller should be held accountable for complying with measures giving effect to the privacy principles, i.e., "accountability."

Multistakeholder Approach -- The OECD is an appropriate forum to consider and develop a globally interoperable digital privacy framework because it recognizes and gives weight to the input of non-governmental stakeholders. Given the rapid pace of technological change, it is critical for business, the technical community, and civil society to advise OECD member governments whether elements of a privacy framework are commercially viable, technically feasible, and offer adequate personal privacy protections. As we have stated in previous submissions, stakeholder inclusion can lower the risk of unintended consequences[4] and increase legitimacy and adoption of policies and regulations.

Evidence-Based Analysis – Equally important, the OECD's evidence-based approach to policy development means that recommendations are based on economic analysis and metrics rather than on political issues or subjective prescriptions. This characteristic of the OECD's work has earned it respect from many non-member countries who likely will use the OECD framework as a model for their respective national approaches.

It comes as no surprise, therefore, that the B20 Digital Economy and Industry 4.0 Task Force (DEI) recommended that the OECD's Privacy Framework be used as a reference to develop greater interoperability in global privacy regimes. "Only a mutual recognition of privacy standards will enable the cross-border flow of data requires for an inclusive digital economy," the B20 DEI report states. [5]

Laying the Groundwork -- USCIB urges NTIA and the U.S. Government more broadly to participate in the OECD's anticipated review of the 2013 Privacy Framework during the 2019-2020 period. We welcome the opportunity to engage with relevant NTIA staff throughout this process. This will enable the U.S. Government and U.S. business to ensure that the revised framework is appropriately refined to address changes in the digital economy during the past five years and is not skewed toward any one country or region's privacy regulations.

[4] For example, business can offer advice concerning possible negative economic, technical or commercial impacts of a proposed policy about which governments may not be aware in proposing the policy.
[5] B20 Digital Economy and Industry 4.0 Task Force Policy Report, p. 54.

In addition, participating in this review may enable outreach to potential country/regional partners in support of using the revised OECD Privacy Framework as a possible mechanism to realize global interoperability.

- *APEC Cross-Border Privacy Rules System (CBPR)* -- For many of the same reasons, USCIB also encourages NTIA to participate in the Data Privacy Subgroup (DPS) of APEC's Electronic Commerce Steering Group (ECSG). Using the OECD's 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[6] and subsequent privacy recommendations as a foundation, the DPS developed the APEC Privacy Framework and Cross-Border Privacy Rules (CBPR) system. The CBPR system requires companies certified by designated authorities to implement data privacy policies consistent with the APEC Privacy Framework, which must be assessed as compliant by an Accountability Agent (the Federal Trade Commission for U.S. companies) and enforceable by law. One of the most promising features of the CBPR is its potential to emerge as a model for regulatory interoperability in the Asia Pacific region and elsewhere.

  Like the OECD Privacy Framework, the principles of the APEC Privacy Framework, comport with the NITA's proposed "Privacy Outcomes." The APEC Framework also recognizes the need for a flexible approach to implementation to accommodate various models of enforcement, the importance of public-private cooperation, and a risk-based approach to selected oversight efforts of Privacy Enforcement Authorities.

  APEC/EU Collaboration -- The European Commission evidently recognized the potential of the CBPR as a model for an interoperable approach to privacy protection. The Commission agreed to work with members of APEC's DPS on a Referential that mapped the similarities of the CBPR to the EU Binding Corporate Rules. Merck, a USCIB member, successfully used the Referential to secure BCR certification.

  The Commission and DPS members followed up the success of the Referential, and currently are involved in a project aimed at mapping the CBPR to the EU General Data Protection Regulation (GDPR). It is important that NTIA coordinate within the interagency process to make sure that NTIA and other U.S. Government staff with privacy expertise participate in this initiative.

  USCIB, which participates in the DPS under the auspices of the International Chamber of Commerce,[7] contributed to the DPS's development of the APEC Privacy Framework and the CBPR. We would welcome the opportunity to engage further with NTIA in shaping APEC's privacy-related work with the European Commission going forward.

  Further, we would be very interested in working with NTIA in developing a proposal to create a mechanism for non-APEC members (from Latin America, for example) to gain certification to participate in the CBPR, possibly via a Memorandum of Understanding (MOU).

---

[6] *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[7] USCIB serves as the U.S. National Committee of the International Chamber of Commerce (ICC). For nearly a decade, the ICC has enjoyed Guest status as a participant in APEC's Electronic Commerce Steering Group (ECSG).

Next Steps: Implementing Interoperability

USCIB proposes a few different approaches aimed at improving the consistency and effectiveness of privacy protection at the global level.

- *Utilize Existing Forums* – In the near-term, there will be prime opportunities at the OECD, APEC and through other regional forums to advance development of international arrangements that promote interoperability among privacy frameworks.
    - *OECD* -- As mentioned, in the 2019-2020 period, the OECD Committee on Digital Economy Policy (CDEP) will undertake a review of the 2013 OECD Privacy Framework. The OECD CDEP likely will convene a special Experts Group to inform the new process. The U.S. Government not only should participate in the Experts Group, but also urge that the Group include all stakeholders as was the case for development of the 2013 Privacy Framework. In addition, we urge the U.S. Government to proactively propose the group's goals and objectives to include specific deliverables aimed at bringing different privacy systems together, *with timelines.*

      For example, a recurring theme in the OECD's privacy work has been the importance of building a strong global network of privacy enforcement authorities as a foundation for global interoperability by enhancing information sharing.[8] The U.S. Government might propose that the biannual CDEP meetings include regular reports from privacy enforcement authorities to enable such information sharing and facilitate coordinated and effective enforcement.[9] This good practice would follow the example of such reporting at the APEC DPS concerning initiatives undertaken under the rubric of the Global Privacy Enforcement Network. That is just one example of a possible interoperability metric.

      Within the OECD Experts Group, the U.S. Government, together with business and other stakeholders, also might encourage consideration of the range of approaches to interoperability among privacy frameworks, such as the EU-US Privacy Shield or the aforementioned APEC CBPR-BCR Referential. The goal would be to identify elements that have proved effective in ensuring privacy protections, while also fostering cross-border data flows and, in turn, attracted government support and private sector participation. In view of political issues that continue to burden the annual renewal of the Privacy Shield framework, the generally well-received APEC-EU Referential may be the less contentious alternative to examine.

    - *APEC* – As mentioned, APEC Privacy Framework has its roots in the OECD's privacy work. However, the APEC economies have been more active and innovative in pursuing interoperable privacy approaches by developing the CBPR system, fostering dialogue among Asia Pacific privacy enforcement authorities, and cooperating with the European Commission on the BCR/CBPR Referential and CBPR/GDPR mapping project. This track-record has increased the attractiveness of the CBPR as a possible model for regional or global regulatory interoperability.

[8] *OECD Privacy Framework, Ibid*., p. 33

[9] The APEC economies have pursued cooperation among privacy enforcement authorities more successfully under the rubric of the CBPR and typically include such reporting at meetings of the Data Privacy Subgroup.

Some observers might argue, however, that the low levels of APEC economy participation and company certification in the CBPR effectively inhibit its emergence as a premier model for regional privacy interoperability. The low levels of participation also raise questions about *why* that is the case. Currently, just six APEC economies participate in the CBPR;[10] 23 companies have been certified, 22 of which are American and one is Japanese.

One reason for low levels of business and government participation in the CBPR system may an insufficient understanding about the potential economic and commercial benefits of having a common "privacy umbrella" for the Asia Pacific region. Asia Pacific economies and businesses also may harbor concerns about the paperwork involved and/or changes to policies and regulations that would have to be undertaken to secure approval.

In addition, we feel it is important to note that in the United States, the FTC is the only enforcement authority for the CBPR. This may inhibit entities that are regulated by the Federal Communications Commission (FCC) from participating in the CBPR, and it may have the same impact on industries regulated by the Department of Transportation.

In any case, the CBPR-participating economies – including the United States -- need to do more within APEC to promote the privacy system to both governments and business through education and outreach. While many privacy experts acknowledge that the CBPR holds promise as an interoperable framework, it is difficult to make the case for its global application when regional participation remains low.

The work underway between members of the APEC Data Privacy Subgroup and the European Commission could effectively demonstrate the broader applicability of the CBPR. We urge the U.S. Government to become actively engaged in that project to ensure that it remains balanced. This project should demonstrate common elements between the two systems, not try to change the CBPR.

If APEC and EU participants can develop a mechanism that would enable dual certification under the CBPR and GDPR -- or at least simplify that effort -- the CBPR will become more attractive to Asia Pacific economies and businesses. Increased participation in the CBPR, in turn, will enhance its credibility as a framework to bring different privacy approaches together globally.

- *Pacific Alliance:* Governments in Latin America continue to respond to data privacy concerns by advancing data privacy bills that unduly restrict the cross-border free flow of data on which modern economies rely. While this is not limited to Pacific Alliance members, we encourage the US Government to actively engage on these issues through the Pacific Alliance.

- *Collaborate with NIST* – It is important that consultations within the OECD and/or APEC clarifying *policy* features of a model for interoperability proceed concurrently and collaboratively with the work of the National Institute of Standards and Technology (NIST). As you know, building upon the success of the multistakeholder process that informed development of NIST's Cybersecurity Framework, in late summer the agency launched a

[10] USA, Mexico, Japan, Canada, Singapore, and South Korea.

similar project to develop a voluntary, risk-based Privacy Framework as an enterprise risk management tool for organizations.

As NIST Director Walter Copan highlighted in recent comments, there currently is a "disconnect between the acknowledged need for better agreement on a shared vision of strong privacy protections and agreed methods for reaching such a vision." He further noted the lack of a "shared lexicon and a practical structure that brings all parties together and is flexible enough to address diverse privacy needs."[11]

Thus, US Government leadership in policy discussions at the OECD, APEC, or other global forums would guide development of the "shared vision." The NIST work, in turn, would establish practical methods to implement the vision. The US Government therefore should pursue the development of a privacy framework in a holistic, whole-of-government fashion. The combined effort will produce a compelling, comprehensive approach, especially for countries that lack the technological capacity to develop implementation tools.

- *Pursue Statutory Changes* – We are aware of growing interest in the U.S. Congress to develop national privacy legislation and we support such legislation. Federal privacy legislation effectively could preempt privacy legislation passed or under consideration at the U.S. state level. Some USCIB members have expressed concerns about the enormous costs and complications of complying with a patchwork of state privacy regulations and have advocated the development of national legislation.

  Federal legislation, properly drafted, could improve upon elements of the GDPR that have complicated U.S. business compliance (i.e., consent-based and right-to-be-forgotten requirements, to name a few), but should not to seek to replicate or "import" the GDPR into U.S. law.

  In terms of building support for a globally interoperable approach to privacy, USCIB urges NTIA to consider the value of national privacy legislation in positioning the United States to be in a stronger negotiating position with the EU and other countries that have argued that US reliance on self-regulation and sector-specific regulations are not "adequate" under their privacy rules. In the same vein, it could provide U.S. negotiators with stakeholder-informed alternatives to problematic provisions, and better enable NTIA to play an effective leadership role.

I. Conclusion

We are grateful to NTIA for this request for public comment to provide the perspective of businesses who are innovators of digital technology on approaches to ensuring a balance between the need to protect consumer privacy, but at the same time pursue innovations, some of which, in turn, will enhance privacy protections. We reiterate that the keys to realizing economic and social benefits in today's digital economy are policies that are informed by *all* stakeholders. Stakeholder guidance and evidence-based analysis will be especially critical to considering how privacy challenges created by emerging technologies, such as Artificial Intelligence, can be shaped to maximize their potential for societal benefits while mitigating possible privacy risks.

[11] Walter G. Copan, Under Secretary of Commerce for Standards and Technology and NIST Director, U.S. Department of Commerce, "Developing the NIST Privacy Framework: How Can A Collaborative Process Help to Manage Privacy Risks?" speech at the Brookings Institution, Washington, DC, September 24, 2018.

We urge NTIA and the US Government to lead efforts to develop a globally interoperable framework for privacy that builds upon the valuable work already undertaken by the OECD and APEC and creates a linkage to the important privacy project underway at NIST.

Sincerely yours,

Barbara P. Wanner
Vice President, ICT Policy

Copies to: Peter M. Robinson, President and CEO
Rob Mulligan, Senior Vice President, Policy and Government Affairs