Supplement on Digital Economy
Enabling the Potential of the Digital Economy
54th Japan-U.S. Business Conference
The U.S.-Japan Business Council / Japan-U.S. Business Council
November 3, 2017

The U.S.-Japan Business Council and Japan-U.S. Business Council (the Councils) see tremendous opportunity surrounding the digital economy, and hope to see the United States and Japan continue to lead the international community in its development. We applaud both governments for the focus they are bringing to digital economy-related issues, support the governments' efforts to share best practices with other countries and regions, and hope for increased dialogues between the U.S., Japan, and others.

To this end, we urge the governments to prioritize the following forward looking public policies related to data and personal information, intellectual property, and the promotion of international standards and best practices related to privacy, cybersecurity, and technical interoperability.

1) Design public policies that will enable new and transformative technologies to benefit society broadly:

The Councils recognize the potential of new technologies, including those linked to Artificial Intelligence (AI) and the sharing economy. We encourage the two governments to continue to welcome these new technologies for their potential economic benefits, and discourage burdensome regulations that might kill new technologies in their infancy. With that said, the Councils recognize that the economic benefits of such technologies may not necessarily be distributed evenly across society, and that certain technologies may affect the labor market in unintended ways.

However, as history has shown us, technological developments have often improved the livelihoods of people. The Councils believe well-designed economic incentives and appropriate public policy can help shape a positive direction for technological change, helping to improve productivity, create higher levels of employment, promote and inclusive growth. To this end, the Councils encourage the two governments to 1) invest in and develop new technologies; 2) educate and train citizens for the jobs of the future; and 3) carefully consider how to best empower workers during the transition to a more automated, digital economy.

2) Establish a safe and secure environment for the use of data and its free movement across borders and avoid data localization mandates:

Given the growing importance of cloud computing and cross border data flows, the U.S. and Japan should work to establish a safe and secure environment for the use of data that serves as a basis for corporate activity without restrictions on locality. The seamless exchange of data across borders and internationally harmonized rules on the protection of personal information will facilitate growth of the digital economy on a global scale. As the two governments consider approaches to address critical privacy and security challenges, it is essential that any such requirements are not made overly prescriptive or one-size-fits-all, do not create barriers to cross-border data flows, and avoid data localization mandates. The Councils ask that the governments be proactive in reinforcing the idea that privacy protection is in no way linked to the physical location of servers or stored data.

To this end, the Councils applaud the leadership demonstrated by the U.S. and Japan with regards to cloud computing. We encourage the two governments to advocate that governments avoid requiring network or data separation for all public institutions utilizing cloud services, thus requiring companies to create separate intranets for these institutions. This approach not only undermines the efficiencies of cloud computing, but makes it prohibitively expensive for companies to build the required physical servers in jurisdictions that cannot leverage the economies of scale of an international infrastructure. This will ultimately deter cloud computing technologies from becoming ubiquitous, and prevent the benefits of the technology from being leveraged on a global scale.

Further, the Councils emphasize the need for a harmonized regulatory framework across all levels of government in both countries, and encourage frequent regulator-to-regulator dialogues between the U.S. and Japanese governments to help achieve this objective. The Councils believe that contradictory and scattered regulations decrease business efficiencies, increase compliance costs, and ultimately impede the development and adoption of new technologies and the growth of the digital economy at large. The need for harmonization is particularly acute in the digital economy, where business models and data flows often fall under the mandates of multiple regulators.

3) Promote internationally harmonized rules and best practices for the protection of personal information:

The Councils applaud the U.S. and Japan for their continued leadership in the promotion of internationally harmonized rules and best practices for the protection of personal information, and in particular in their continued promotion of these ideals

through the APEC Cross Border Privacy Rules system (APEC CBPR). In the absence of the cutting edge rules for digital trade, privacy, and cross-border data flows agreed upon under the Trans Pacific Partnership, the APEC CBPR has become one of the few multilateral tools that U.S. and Japanese companies have to ensure competiveness in Asia's dynamic marketplace.

We welcome the recent discussions between APEC members and the European Union on interoperability between CBPR and the EU's General Data Protection Regulation (GDPR). We urge the U.S. and Japan to continue to lead in creating a future work plan, particularly as Japan and the EU work towards mutual adequacy decisions on international data transfers. There is great room for U.S.-Japan collaboration in spreading such rules and practices throughout the Asia-Pacific through trade agreements, APEC processes, and other platforms. We urge the governments to identify such opportunities in concert with the private sector.

Similarly, The Councils are encouraged by Japan's continued efforts to pursue the cutting edge rules for digital trade, privacy, and cross-border data flows agreed upon under the Trans Pacific Partnership, and hopeful that Japan will continue to promote these high-standards on a regional and global scale.

4) Prioritize connectivity and the further development of digital infrastructure:

The Councils urge the two governments to continue to prioritize the development of digital infrastructure that will be required for future growth, and the realization of the benefits associated with "the 4th Industrial Revolution" or "Society 5.0". We encourage the two governments to continue efforts to facilitate international payments and transactions and make the Internet a truly seamless commercial platform, and importantly to prioritize connectivity. The Councils believe the deployment of ultrahigh-speed Internet Protocol networks will be a critical component to the development of the digital economy, and importantly serve as a "backbone" to some of the most promising technologies of the future.

5) Protect Intellectual Property:

Protection and enforcement of intellectual property rights remain the foundation of innovation and are key to the realization of the potential of the digital economy. The Councils encourage regular consultation between the two governments and the private sectors to ensure that intellectual property protection laws and regulations adequately support and protect existing rights, as well as the new ideas and business models that will emerge from ICT technologies.

Further, the Councils consider proper and legal usage of intellectual property essential for economic growth, and urge both governments to promote balanced policies of protection and usage of IP. The Councils believe that security requirements should not mandate forced technology transfer or review of IP such as source code. Such IP is business proprietary information that is essential to a company' ability to innovate and remain economically competitive. These requirements are problematic for ICT firms that (i) are already struggling to protect their intellectual property, and (ii) may have licensing obligations that preclude the disclosure of such code to customers in other countries who would be deeply concerned about possible security issues if a foreign government is given access to the code. Trade-inhibiting security reviews for ICT products and services may not only weaken security and constitute technical barriers to trade as defined by the WTO, but also reduce incentives to innovate.

6) Avoid country-specific regulations or requirements and develop voluntary, industry-led, and consensus-driven standards:

The Councils are concerned with the increase in country-specific government mandates relating to the digital economy – including privacy and cybersecurity requirements, technical standards, and interoperability. We believe such policies hinder U.S. and Japanese firms' ability to operate in external markets, limit the positive effects of competition, and are a substantial obstacle to the full realization of the digital economy's transformative potential. In contrast, technologies built on global standards combined with globally consistent regulations can boost innovation and competition, and will ultimately improve the lives of consumers across the globe.

The Councils also emphasize the importance of voluntary, industry-led, and consensus-driven standards developed through transparent and impartial processes, and focused on market-driven outcomes. A competitive environment that uses technology neutral frameworks will allow the digital economy to be leveraged in the most efficient manner, and will help prevent competition policy from being used to achieve industrial policy goals.

The Councils believe that the role of government should be to 1) encourage the development and adoption of standards related to the digital economy and emerging connected technologies, 2) foster interoperability in an open and transparent manner, and 3) participate in the standards setting process as a convener, trusted expert, and major purchaser and implementer of standards, but avoid "picking winners".

7) Increase U.S.-Japan collaboration on cybersecurity in international fora:

Given the nature of cyber threats, the Councils reaffirm their support for globally-aligned approaches to cybersecurity that advance cybersecurity and keep pace with the constant evolution of cyber threats. In international fora, the Councils encourage the U.S. and Japanese governments to:

1) Promote a flexible, innovation-enabling approach to cybersecurity;
2) Harness the convening power of government to increase public-private collaboration;
3) Prioritize risk management as the basis for enhancing cybersecurity;
4) Utilize international standards to enable the deployment of best-in-class approaches to cybersecurity across borders; and
5) Embrace opportunities for international cooperation and coordination.

7.2) Encourage cyber threat information sharing to increase cyber resilience:

The Councils recognize the potential for cyber threat information sharing to increase cyber resilience in the U.S. and Japan, by providing advanced warning of potential threats and their characteristics. Given that critical infrastructure is often operated by private entities, it is critical that they be incorporated into information sharing initiatives. The Councils encourage the U.S. and Japanese governments to:

1) Employ international information sharing standards and protocols;
2) Implement sufficient liability protections for companies who share threat information;
3) Provide incentives for companies to expand engagement in information sharing entities; and
4) Be transparent and conservative about how information shared with government entities can be used by law enforcement agencies.

7.3) Promote cybersecurity in the Internet of Things (IoT):

With 20 billion connected devices estimated to be in use by 2020, the Councils recognize the importance of cybersecurity of such devices in preventing large scale attacks. Regulators should be cognizant, however, of the limitations of top-down regulation of IoT security and the need to avoid prescriptive solutions that hamper innovation. The Councils have adopted the following principles, which they encourage regulators to embrace:

1) Promote technical compatibility and interoperability, to ensure that political boundaries do not become obstacles to the movement of devices, data, or IoT-related services;

2) Leverage international standards to promote common approaches and solutions; and

3) Encourage the development of richer interactions between devices and the network so that machine learning and automation can be leveraged to manage at the endpoints more effectively.