PACIFIC FORUM

Key Findings
United States-Singapore Cyber & Tech Security Virtual Series
Session #5: US-Singapore Perspectives on
Strengthening Digital Data Governance
March 10, 2021 (US) | March 11, 2021 (Singapore)

On March 10, 2021, with the support from the US Embassy Singapore, the Pacific Forum hosted "US-Singapore Perspectives on Strengthening Digital Data Governance," with 42 participants from the government, private sector, academia, and other non-governmental organizations. This was the fifth session in the United States-Singapore Cyber&Tech Security Virtual Series.

Dr. Nicol Turner Lee, the Senior Fellow in Governance Studies and Director of the Center for Technology Innovation at the Brookings Institution, and Evelyn Goh, Director, International Policy & Strategy, Infocomm Media Development Authority (IMDA), Singapore, examined the different mechanisms that the US and Singapore have adopted to strengthen digital data governance to safeguard data privacy and promote innovation.

Key findings from this meeting are described below.

Digital Data Governance in Singapore

The 2012 Personal Data Protection Act (PDPA) is the main data protection legislation in Singapore governing the collection, use, and disclosure of individuals' personal data by organizations. In November 2020, the PDPA was amended to increase accountability, enhance enforcement, provide consumer autonomy, and support innovation in a rapidly evolving digital landscape. For example, the PDPA now provides for higher penalties in cases of non-compliance, and introduced data breach notification and data portability obligations, putting individuals in greater control of their personal data.

In 2019, Singapore introduced the Data Protection Trustmark Certification, through which businesses and consumers can identify organizations with accountable data management practices. It is a voluntary certification that can play an important role in increasing a company's competitive advantage and helping to build trust between companies and consumers. IMDA also helps organizations by providing a DPTM Certification Checklist for them to self-assess their readiness.

At the international level, Singapore has committed to Memorandums of Understanding, Free Trade Agreements, and Digital Economy Agreements which include provisions on personal information protection and cross-border data flows. Singapore is part of the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system, a multi-lateral data privacy certification that companies can join to demonstrate compliance with a set of APEC-approved requirements. CBPR-certified companies are recognized by other APEC participating economies, facilitating the flow of data across borders. In Singapore, the Infocomm Media Development Authority (IMDA) is appointed as the APEC CBPR accountability agent.

ASEAN has adopted a two-pronged approach to facilitate data flows across the region, ASEAN has recently developed and adopted a set of Model Contractual Clauses (MCCs). The MCCs are useful for businesses transferring personal data and help businesses reduce lengthy contract negotiations. The next step for the region is to develop an ASEAN certification.

In Singapore, the Personal Data Protection Commission provides guidance on the application of the PDPA through advisory guidelines and has also developed different tools for businesses to help them with compliance such as the PDPA Assessment Tool for Organizations. There is also a great deal of outreach to consumers to help them understand what information can be collected about them.

In the context of Artificial Intelligence (AI), Singapore’s data governance complements its national AI strategy which is overseen by Singapore’s National AI Office. IMDA has developed the Model AI Governance Framework and the Implementation and Self-Assessment Guide for Organizations, which are practical tools for companies to deploy AI responsibly.

Digital Data Governance in the US

In the attempt to harmonize data governance domestically and internationally, data privacy poses important challenges. As of today, the US has no federal data privacy regulations for handling and sharing data. Overall, despite international membership in mechanisms such as APEC's CBPR, data privacy standards remain a largely underexplored area in the US.

Due to the current pandemic, we are learning that the lack of shared data privacy standards can lead to an increase in hostile activities, such as information surveillance. Such threats require the development of relevant and comprehensive structures, such as the General Data Protection Regulation (GDPR) in the European Union (EU).

In the US, data owners have not been clearly defined. Ownership of data is going to be a central part of the debate on data privacy standards in the US. Existing regimes, such as the EU GDPR and California’s data privacy legislation, identify *consumers* as the ultimate owners of data. Such differences show that data privacy regulations go beyond matters of trade and include core values and principles, making it hard to reach a consensus on shared standards.

Data standards are important to avert the possibility of biased data and/or misuse of personal data, which creates differential treatments. The absence of national standards can have a negative impact on civil rights, as has been shown by the algorithms embedded in facial recognition technologies used by some police departments in the US, creating racial bias.

Fortunately, the data privacy debate in the US is taking place and there are increasing efforts to enhance accountability and enforcement by regulatory authorities through penalties and potential new avenues for litigation.

It is important for the US to catch up with the rest of the world for several reasons. The digital economy has changed and will become increasingly more dependent on data in different ways, especially in data-intensive industries such as AI and 5G. These developments will require strong national legislation as well as cross-border cooperation to reduce ambiguities in data flow regulations.

The Role of the Private Sector

Big tech companies should be managed based on three verticals: (1) Prescriptive – which includes the compliance and regulatory regimes that dictate what is permissible for matters such as sharing, retention, and repurposing of data; (2) Self-regulating – which refers to what companies can do to be more responsible actors in areas such as differential privacy – a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset – as well as privacy by design, where privacy is built in the backbone of applications, reducing risks; and (3) Adaptive – how to ensure that there is minimum harm to consumers in an ever-changing environment that constantly creates blind spots. Issues such as the use of facial recognition systems and other biometrics data present several challenges that are being dealt with in different ways around the world.

US-Singapore Cooperation

The next step for ASEAN is to fully implement the MCC. ASEAN is also developing a region-wide certification to facilitate data flow across ASEAN member states. For the US, there is a need to revisit policies from the Obama administration on data privacy and governance, specifically on data sharing and portability.

Moving forward, the US and Singapore should continue to embrace and improve the APEC CPBR. This effort should include more capacity-building measures to close the digital gap and deal with differing levels of digital maturity within ASEAN. Globally, there is an urgent need to regulate big tech companies and establish reciprocal and exportable models to address AI bias.

This document was prepared by Eugenio Benincasa and Mark Manantan. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Director of Nonproliferation, Technology, and Fellowships at Pacific Forum. These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.