

Address by Under Secretary McIntosh at the Sim Kee Boon Institute for Financial Economics at Singapore Management University:

February 5, 2020

As prepared for delivery:

10:30 a.m. SGT

February 6, 2020

Singapore

INTRODUCTION

Good morning. Thank you all for being here today to discuss the important and timely topic of data connectivity in financial services. I'm glad to be here in Southeast Asia, a diverse, vibrant, and economically critical part of the world. The United States has long been a close friend and major business partner of ASEAN, a regional bloc that distinguishes itself in having the largest cumulative U.S. direct investment stock in Asia.

It is particularly fitting to address today's topic in Singapore. As a critical financial hub for the region and the world, Singapore is a prime example of how the ability to move and access data across borders – to connect to other markets – can contribute to economic growth and development. The ASEAN region also has a dynamic, fast-growing digital economy that is offering innovative financial services to a mobile-savvy population. The United States looks forward to exploring new avenues for collaboration on financial innovation and data connectivity with our ASEAN partners.

We view “data connectivity” as the process of how, working across borders, firms connect to their customers, manage risks, commercialize data value, and provide information, including to the government authorities that supervise them. Data connectivity is a complex and multi-dimensional issue with important implications for the financial services sector. My friend Ravi Menon, Managing Director of the Monetary Authority of Singapore, is an authority and thought leader in this area [I understand that unfortunately he is traveling and could not be here today]. Today I'd like to pick up the conversation that Ravi helped start a few years ago and lay out a vision of how public authorities can work together to realize the benefits of enhanced data connectivity in financial services.

Data connectivity translates directly to demonstrable economic growth, and has for years. In 2014, cross-border data flows added approximately \$2.8 trillion dollars to global GDP, surpassing the impact of the goods trade.^[1] Today, data connectivity is transforming the delivery of financial services by enabling new products and services, increasing consumer access, and facilitating value chain efficiency.

It is also essential to supporting financial stability. In recognition of the importance of the financial sector's contribution to the “plumbing” of the economy, financial sector authorities have specific data access needs that allow us to effectively do our jobs. Data connectivity facilitates financial regulators' access to the financial risk-related data needed to fulfil their mandates in ensuring safety and soundness. In turn, financial authorities have decades of experience handling market sensitive and personal data, managing cross-border information-sharing arrangements, and safeguarding financial data privacy.

When data connectivity is impeded, firms, consumers, regulators, and the economy as a whole are all worse off, and we risk losing out on many benefits of today's digital economy. Effective data governance policies should take into account considerations of the financial services market and existing regulatory data requirements aimed at promoting financial stability and market integrity. It is becoming increasingly clear that a “one-size-fits-all” approach is not optimal. To be sure, there are difficult public policy issues in play, with no off-the-shelf answers, but we as policymakers have an obligation to ensure that our economies can reap the benefits of data connectivity. Financial authorities, in particular, need to step up our engagement on data governance issues.

To that end, the U.S. Department of the Treasury is enhancing our efforts to support data connectivity. From trade agreements to financial regulatory cooperation, we are focused on how we can work, on a bilateral and multilateral basis, to harness the benefits of cross-border data flows. Consistent with these efforts, I am pleased that earlier today, the United States and Singapore issued a joint statement laying out our shared views on data connectivity in financial services.

CROSS-BORDER DATA AND GROWTH: PROMOTING INNOVATION AND COMPETITION

Before we delve into the opportunities and challenges we now face with data connectivity, I thought I'd spend a few minutes on the evolution of financial services. The ability to securely hold and transfer financial information has always been essential to the safe and efficient provision of financial services – and the sector's growth and innovation is intensely data-driven.

The dramatic increase of internet availability and improvements to internet architecture have spawned a generation of consumers that expect financial services to be as seamless and immediate as email and social media.

These new applications of financial services and the technology underpinning them are inherently international. They depend on geographically diverse ecosystems of software, hardware, and financial intermediation providers. Working together, across borders, these distributed ecosystems offer innovative services more quickly and at lower cost, increasing financial inclusion and consumer choice while increasing productivity and driving economic growth.

In a global economy, financial innovation increasingly depends on the ability to make financial data available and accessible, including across borders. Since 2012, almost two billion people have gained access to the internet, from 2.5 billion in 2012, to 4.4 billion in 2019 – with over 360 million users in Southeast Asia alone.^[2] With more than half of ASEAN member states' citizens still unbanked,^[3] small and medium size enterprises – and other innovative providers – are poised to leverage mobile technology to provide consumers with their first experience with payment services, insurance, or savings accounts. The untapped potential of this market could drive the next century of growth across ASEAN and the rest of the global economy.

Today, much of the computing power a financial services firm uses is outside its physical building. Many firms, especially smaller ones, rely on the power and flexibility of innovative infrastructures like distributed computing – the cloud – which allows companies to reduce costs by accessing computing power commensurate with their business needs, rather than requiring investment in on premise hardware and infrastructure. This technology is especially helpful to both small and medium-sized enterprises.

The opportunities the cloud presents clearly demonstrate how data connectivity supports productivity growth by helping firms allocate labor and capital efficiently. Cloud computing also democratizes access to artificial intelligence and big data analytics, which can help shift human capital to non-routine tasks. According to some estimates, 20 percent of non-routine tasks generate 80 percent of value creation.^[4]

The power of this distributed infrastructure undergirds the promise of digital banking in the ASEAN region. Here, firms are starting natively on the cloud, which allows them to provide services in multiple jurisdictions without needing to build physical bank branches or install and maintain their own costly computing infrastructure. These banks and other digital financial services currently generate \$11 billion in revenue in the ASEAN region; that number has the potential to grow threefold to \$38 billion by 2025, accounting for 11 percent of total financial services revenue.^[5]

Authorities across the region are also stepping up their game, leveraging financial innovation to increase competition and boost sustainable economic growth. Authorities and firms are looking into the possibility of making significant improvements to the cost and efficiency of cross-border payments and trade financing using digital ledger technology. Others are looking into developing more flexible credit scoring and credit history models to boost financial access.

The United States welcomes financial innovation in the ASEAN region and the opportunity for cross-border collaboration. Economic growth is not a zero-sum proposition. When jurisdictions make their business environments more attractive for trade and investment, everyone – individuals, firms, and governments – will benefit. Competition drives innovation and better outcomes for consumers.

I think we have to attribute some of the vibrancy in the ASEAN fintech market to competition and the ability of startups and other firms to offer services in multiple markets in the region without building physical branches or computing infrastructure to reach their customers. In Southeast Asia, at least 100 fintech firms are already operating in two or more ASEAN markets,^[6] and many others surely

plan to expand. Digital financial services of this century will only realize their full potential if we can establish effective cross-border data policies, precisely because these firms are innately borderless and frequently derive value from the ability to harness data effectively.

CROSS-BORDER DATA AND FINANCIAL STABILITY

At the same time, innovation will also require firms to revisit existing risk management practices, and authorities to reassess existing regulatory and supervisory approaches. New technologies with global reach may pose risks that require enhanced cross-border information sharing and collaboration among authorities, and multi-jurisdictional risk management practices by firms. Here, too, data connectivity is essential.

Firms that operate in more than one jurisdiction need to ensure that they can assess, aggregate, and manage financial risks consistently and comprehensively across jurisdictions. This includes banks operating outside their home market, which provide, on average, 15 to 20 percent of the total credit to emerging markets, with particularly strong connections in closely-knit regional markets, such as Latin America and Southeast Asia. Firms also address operational risks holistically, across the entirety of their operations, seeking to optimize their use of infrastructure – including the number and location of data centers, reliance on third-party hardware and software vendors, and reliance on innovative cybersecurity solutions, in the cloud or otherwise – for maximum resiliency and security. We as policymakers care a great deal about the ability of these firms to manage risk, given the interconnected nature of financial markets and potential for risks in one jurisdiction to propagate quickly across borders.

In one example that is now well-known, as Lehman Brothers was heading to bankruptcy in 2008, the major international banks lacked the granular data needed to quickly measure domestic and cross-border exposures to a possible Lehman failure. Exposure to Lehman didn't include only direct exposure from Lehman investments, but also counterparty risk from ongoing derivatives trades in multiple jurisdictions with different Lehman subsidiaries. After Lehman's collapse, firms were unable to even identify counterparties effectively and share this information across borders, which eroded confidence in the system and made addressing the systemic risks impractical. Since then, G20 reforms led by the Financial Stability Board have sought to improve transparency in derivative markets and standardize counterparty identification. This event crystallized the importance of timely and accurate cross-border data flows to global risk management.

For financial regulators and supervisors, data connectivity is also essential to obtain the information they need to fulfill their mandates and promote the safety and soundness of the financial system – and by extension the overall health of the economy. Banking regulators, for example, need access to consolidated and transaction-level data to confirm that a firm's financial statements are accurate and that its balance sheet reflects compliance with capital and liquidity standards and prudent risk management. When it comes to investor protection standards, assessing compliance can require reviews of disclosures relating to fees, expenses, and conflicts of interest. And in today's global economy, the provision of financial services often includes a cross-border component, requiring regulatory access to information in other jurisdictions to effectively monitor potential risks.

Financial regulators need to cooperate with each other in today's digital economy, and that includes sharing data where appropriate. Regulatory authorities in the United States and here in Singapore have a number of bilateral information-sharing arrangements and are parties, with other jurisdictions, to a range of multilateral information sharing arrangements. All told, the United States has over a dozen of these arrangements with regulators across Asia – and many more around the globe.

I was pleased that just last year, the U.S. Department of the Treasury was able to expand cooperation in the insurance sector through a comprehensive memorandum of understanding on information sharing with the insurance supervisor in India. These relationships are extremely important, and we must continue to emphasize the need for greater clarity and understanding around cross-border information sharing among regulators.

RISKS FROM DATA RESTRICTIVE POLICIES

Data localization – measures that require at least some data to be hosted on local data servers or restrict the transfer of data outside national borders – is one example of a policy that challenges the immense benefits of data connectivity. Such measures have proliferated in recent years. In some cases, these policies are crafted with industrial policy aims in mind. In other instances, they are meant to address legitimate public policy concerns related to privacy, cybersecurity, and regulatory and supervisory access. In my view,

there is no inherent trade-off between achieving those public objectives and the benefits of economic growth and financial stability associated with data connectivity.

Just as data connectivity supports growth and innovation, there is a growing body of evidence that forced data localization imposes economic costs, especially in emerging economies. For example, one study found that economy-wide data localization requirements could decrease GDP between 0.7 to 1.1 percent and lower domestic investment between 0.5 and 4.2 percent.[7] Another recent analysis found a clear, negative relationship between restrictive cross-border data policies and the quantity of imported services,[8] which could, among other things, limit access to innovative financial services for consumers and firms.

These kinds of restrictive data policies can cut off innovative companies from their customers and prevent them from partnering with the larger ecosystem of financial services providers by limiting their ability to utilize digital infrastructure. Restrictive data policies may, for example, limit the ability of firms to store their data on cloud servers outside their jurisdictions. This is particularly damaging for small and medium-size enterprises that lack the capital budget to develop their own on-premise IT infrastructure. Limiting cloud adoption will damage these firms' ability to leverage the big data analytics, cybersecurity, and innovative tools that cloud services have democratized.

Data restrictive policies, including requirements to store a local copy of data in a particular jurisdiction, also threaten to weaken risk management practices. The potential effects on cybersecurity alone are worthy of serious attention. Requiring an artificially inflated number of data centers increases the number of physical access points for bad actors, without countervailing benefits to resiliency. Policies that dictate the location of data centers can reduce the ability of firms to optimize the system-wide resiliency of their computing infrastructure and can lead to greater exposure to geographic-specific risks, like those posed by natural disasters. While no one doubts the importance of well-planned redundancy to mitigate operational risk, artificially mandated redundancy can actually multiply operational risk. And siloed data storage can be even worse, preventing firms from analyzing data on a global basis, which is critical not only to assessing financial risks, but also to managing and mitigating operational risks.

Critically, to combat money laundering and terrorist financing threats, firms have an obligation to analyze transaction data and identify suspicious transactions to report to the appropriate authorities. This requires consolidated and comprehensive data sets that reflect a complete profile of each customer and their transactions – including those that cross borders.

Similarly, while it is true that all financial regulators require access to data for regulatory and supervisory purposes, data-restrictive policies impede rather than ensure that access. In a world in which data localization measures become more prevalent, financial regulators will find themselves in the midst of a race to the bottom where access to data needed for regulatory and supervisory purposes becomes more difficult for all regulators. Most regulators and supervisors, including our own in the United States, are able to obtain access to the data they need without requiring local storage and processing in nearly all circumstances. For example, in some instances, financial regulators can access data directly from financial institutions through an electronic portal. We all know that physical access to a computer does not equal access to the data on that computer, and access to the data does not require physical access to the computer, so we should work together to ensure that data access is available to all regulators and supervisors that require it.

Impediments to data sharing can also challenge the efficacy of the dense patchwork of cross-border regulatory and supervisory arrangements that jurisdictions worked so hard to develop following the Global Financial Crisis. If data is further fragmented, will we be able to utilize these tools in a crisis? Will financial sector authorities in regional markets, such as Southeast Asia, be able to develop similar tools? In a worst-case scenario, will the failure to maintain data connectivity undermine the significant strides we've made with post-crisis reforms?

We need to consider these questions carefully as we design cross-border data policies in the financial sector and not head down a path of data fragmentation, with reduced outcomes for innovation, inclusion, and financial stability.

A CALL TO ACTION

The continuing march toward digitalization of financial services – and away from physical bank branches – presents a wide array of opportunities, but also new and complex risks. So where does that leave us?

As policymakers we need to work together in addressing two key questions if we are to reap the benefits of innovation and avoid a slide toward data fragmentation:

First, how can financial authorities facilitate an environment open to innovation – innovation that is increasingly dependent on the ability to harness data, including cross-border data – while preserving core public policy objectives such as data privacy, security, and financial stability? And what does an ideal end-state look like?

Second, what does effective cross-border collaboration look like in this space – and what can financial services policymakers be doing to leverage existing mechanisms and work together in new ways on these issues?

On the first question, as to what an ideal end-state might look like, our common objectives outweigh possible areas of difference. For example, I believe we can all agree that:

- Financial innovation depends on the ability to make financial data available and accessible, including across borders.
- Policymakers should increase efforts to promote an environment conducive to innovation.
- And the security and privacy of customer data is essential, including in the context of cross-border data flows. This means at a minimum that: there should be greater cooperation among different functional authorities with oversight in areas such as data privacy, security, and financial regulation; and financial institutions should be transparent in disclosing their data policies.

Likewise, to promote financial stability:

- First, financial sector authorities should have access to information, including on a cross-border basis, to fulfill their regulatory and supervisory mandates.
- Second, robust risk management practices are essential to the functioning of the financial system, and for these practices to be effective, firms must be able to incorporate data about business operations and activities across borders.
- And, third, public policy should enable firms to optimize their infrastructure and operations to achieve optimal resiliency and security outcomes.

I want to re-emphasize that there are no inherent trade-offs among these objectives. Securing supervisory access, for example, need not detract from efforts to facilitate innovation. I also want to underscore again that policies that restrict data connectivity jeopardize these objectives of promoting innovation and stability in financial services, and can lead to unintended, negative consequences. Achieving these objectives in tandem will require close cooperation and consideration among financial authorities. It will also require that we work well with other policymakers outside the financial services world, given that some of these issues have broader implications for the economy.

As for the second question I posed, on how to work together on achieving our shared objectives, we need a more strategic approach to strengthening cooperation. Agreements with trading partners are a strong starting point, and we can build on this good work. But financial authorities should recognize that the importance of data connectivity extends far beyond trade. We need to prioritize engagement on this subject. This means raising awareness of these issues and encouraging multilateral forums to take them on, as well as heightening bilateral engagement with like-minded countries.

In the trade space, beginning in 1997, with the WTO Understanding on Commitments in Financial Services, a growing number of countries have committed to allowing cross-border transfers of information in financial services. The United States and others, including a diverse array of parties such as Australia, Japan, Hong Kong, Mexico, and Canada have included provisions in trade agreements that enhanced these data connectivity protections by prohibiting data localization – including prohibiting requirements to “mirror” copies of information locally – in instances where regulators have access to data for regulatory and supervisory purposes.

Although these trade obligations can provide certain baseline assurances, ultimately they do not answer many of the more complex and novel questions that financial regulators and other policymakers increasingly encounter. To answer those questions, we need to look for opportunities to strengthen cooperation among financial regulators.

There are opportunities to push this conversation forward within multilateral forums, with a foundation of existing work in some areas. For example, financial sector authorities are sharing regulatory objectives related to emerging issues in the financial sector. Financial Stability Board members are developing a toolkit of effective practices for financial institutions and authorities to respond and recover

from a cyber incident. Authorities have also started to consider the state of existing regulatory practices for outsourcing arrangements at the FSB, IOSCO, and the Basel Committee.

As part of our G7 Presidency in 2020, the United States is establishing a technical experts group on cross-border data issues in financial services. The group will aim to foster a sharper understanding of the key public policy objectives at issue, including many of those mentioned today, with the goal of creating stronger communication channels with relevant counterparts.

There is also significant potential for bilateral cooperation, both with countries that share a common understanding on these issues and with those that may not share our views. The U.S. – Singapore Joint Statement on Financial Services Data Connectivity affirms the approach on data connectivity laid out today while also recognizing the need for greater cooperation on these issues. We look forward to carrying forward this work with our colleagues at MAS and finding opportunities to engage with other jurisdictions based on our shared understanding. There is also an important role for like-minded countries to play in reaching out to those jurisdictions that have implemented data restrictive policies to engage in candid discussions on the risk these policies pose to financial stability and economic growth, and alternatives that achieve our common goals. I can tell you that this is a regular agenda item in my discussions with foreign counterparts.

Of course, financial authorities do not have all the answers on data governance. Many questions here are economy- and society-wide, and require discussions with privacy authorities, cybersecurity experts, market participants, and other relevant experts. But financial authorities do have a distinct role to play. With the expertise financial sector authorities bring to the table on data connectivity, and what is at stake for the sector, we need to accelerate our engagement to identify potential solutions. We urge other financial authorities to join us in jumping faster – and deeper – into the conversation. We look forward to working with other governments, market participants, and other stakeholders to tackle these challenges, and to identifying areas of common understanding to achieve the benefits of greater cross-border data connectivity.

Thank you.

[1] McKinsey Global Institute, [Digital Globalization: The New Era of Global Flows \(Mar. 2016\)](#),

<https://www.mckinsey.com/-/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx>.

[2] Reuters, [Southeast Asia's Internet Economy to Hit 100 Billion this year](#), Oct. 3, 2019.

[3] World Bank, [The Global Findex Database](#).

[4] Accenture, [Why is Artificial Intelligence Important?](#) 

[5] Bain & Co, Google, and Temasek, [E-Conomy SEA 2019](#) 

[6] United Overseas Bank, PWC, Singapore Fintech Association, [Fintech in ASEAN: From Start-up to Scale-up](#)

[7] The European Center for International Political Economy (EICPE), [The Costs of Data Localization: A Friendly Fire on Economic Recovery](#) 

[8] EICPE, [Do Data Policy Restrictions Inhibit Trade in Services?](#) 