ADVISORY GROUP
PAPER 3B PRESENTATION

Document: AGFSCB 38-015B
Draft: **SECOND**
Date: 22 July 2018
Source: AGFSCB Chair
Meeting: Kuala Lumpur, Malaysia

An APEC Roadmap for a New Financial Services Data Ecosystem

Outline

- Executive Summary
- Introduction
- General Data Regulation
- Cross-Border Data Flows
- Conclusion (short – to be added later)

Annexes

A. Principles – APEC compared with OECD
B. Conference speakers and conference call participants
C. Singapore conference agenda

Introduction

- Data revolution – volume, velocity, capacity, demand
- Data – role in financial services and inclusion
- Technologies behind data revolution
- Potential for misuse
- Landscape
  - Technology and industry landscape
  - Legal and regulatory landscape

General Data Regulation

General Data Regulation

- Core principles
  - APEC Privacy Framework and OECD
- Consistency of laws and regulations within each jurisdiction
  - Promote consistency, review, reform, reach out
- Expanding the collection and sharing of data
  - Full-file and comprehensive
    - Traditional data – Structured
    - Alternative (non-traditional) – Structured + Unstructured
    - Promote full-file and comprehensive, collect more data, regulatory framework
  - Uses of unstructured data (Big Data) and industry regulation
    - Balanced regulation, separate from credit bureaus
    - Own law + regulator + ecosystem

General Data Regulation

- Creating Sound Frameworks for Collection, Storage, Sharing, Use of Data
  - Data protection and privacy
  - Consumer consent and use
  - Data and derived data: rights and responsibilities
  - Level Playing Field
  - Algorithms – ensuring trust
  - Help regulators improve understanding
  - Regulator+ industry+ financial education
  - Review adequacy of laws/regulations
    - Proactive, holistic, system
    - Principles-based approach + industry codes of conduct
    - Proportionate and flexible
    - Focus on misuse of data and harm to consumers
    - Level playing field

Cross-Border Data Flows

Cross-Border Data Flows

- Addressing concerns behind localization
  - Identify concerns, better options?
- Data privacy
  - Gap analysis – CBPR/APF=GDPR and Individual economies=CBPR/APF
  - Broader industry participation in CBPR – reduce costs for MSMEs, certification mark
- Data security
  - APEC: Long-term strategy
    - Guidelines, intelligence sharing, innovation, sandbox, incentivize boards, leverage expertise and resources
  - Individual economies: review laws, reform law + industry best practices

Cross-Border Data Flows

- Access to data for law enforcement
  - Reform Mutual Legal Assistance Treaty (MLAT)
  - Bilateral/plurilateral agreements
- Domestic data infrastructure and data driven industry
  - Holistic, education, invest in digital infra
  - APEC Blueprint and APEC Best Practices

ADVISORY GROUP
MEETING PAPER 3-B

An APEC Roadmap for a New Financial Services Data Ecosystem

TABLE OF CONTENTS

ADVISORY GROUP
MEETING PAPER 3-B

An APEC Roadmap for a New Financial Services Data Ecosystem

EXECUTIVE SUMMARY

Ensuring progress in harnessing the potential of technology and data to achieve greater financial inclusion and efficiency calls for efforts within APEC to develop a shared vision of a future data ecosystem and to collaborate in achieving this. It requires clearer awareness that laws and regulations taken in response to concerns, such as those about data privacy and security, have consequences on the costs of financial services. Toward this end, key stakeholders from the private and public sectors and multilateral and academic institutions, using the Asia-Pacific Financial Forum (APFF) under the leadership of the APEC Business Advisory Council (ABAC) as a platform, collaborated to undertake a series of conference calls and a conference in Singapore to create this Roadmap. [*See Appendices A and B for the list of participants and speakers and the conference program.*]

This Roadmap identifies critical building blocks of an enabling data ecosystem for the region and outlines concrete initiatives and actions to put these building blocks in place over a reasonable time frame. It provides a tool for promoting consistency of laws, policies and regulations in APEC economies with existing internationally agreed principles, frameworks and good practices, and identifies areas where new minimum benchmarks need to be developed in order to achieve regional consistency. It also points out key considerations and the way forward for individual jurisdictions to undertake reforms and for regional cooperation to be harnessed for the purpose of promoting expanded collection, sharing and use of data within and across jurisdictions leading to greater inclusiveness and efficiency of financial services in the region.

General Data Regulation

In developing data protection laws and regulations that meet the specific needs of their respective jurisdictions, economies should strive for consistency with the *APEC Privacy Framework*, the Basic Principles under the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, and the World Bank's *Good Practices for Financial Consumer Protection*.

Economies should promote consistency among the variety of domestic laws, policies and regulations within their respective jurisdictions impacting the generation, collection, storage, sharing and use of data across central-level ministries and agencies and different levels of government, by reviewing these laws, policies and regulations in collaboration with the financial industry, enterprises and consumers, and undertake changes where needed to reinforce agreed objectives.

Economies should foster a credit information system that is both full-file (based on both positive and negative credit data) and comprehensive (using both traditional and alternative data), by taking steps to improve the availability and accuracy of information and expand the sharing of credit information from various sources, including public data sources. They should collaborate to promote regional consistency of their domestic systems and support future cross-border sharing of credit information. They should also review their legal and regulatory frameworks for credit reporting and undertake improvements where needed, referencing the World Bank's *General Principles for Credit Reporting* as appropriate.

Emerging markets should adopt a balanced regulatory approach toward the new data and analytics industry that fosters continued innovation and inclusion while also protecting consumers and financial system integrity. They should strive toward developing and/or

maintaining a comprehensive and dedicated law or an over-arching regulation on personal data protection that reflects this approach, and establish where needed a general personal data regulator that has capacity to implement and power to enforce personal data protection in parallel with established financial regulators. The data ecosystem should also include an independent industry association and practice codes of conduct; efficient and low-cost complaint, correction and dispute resolution mechanisms, particularly out-of-court procedures; rules governing cross-border data cooperation, investigations and data flows; and specific financial sector regulations and guidelines for firms providing financial services. As the largest holder of data in the economy, government should stimulate the growth of the market by making public data available in a convenient manner for pre-approved legitimate business purposes.

In addition to alignment on key principles like transparency, open data and interoperability, APEC should undertake capacity building activities to help relevant policy makers and regulators deepen their understanding of the changing data technology and industry landscape and enhance their readiness to undertake policy reforms. It will also help them to effectively engage with data service providers in ensuring their compliance with laws and regulations and to be able to make good judgments on the soundness, inclusiveness and fairness of their operating models, methodologies and algorithms and provide effective guidance.

Regulators should collaborate with industry to facilitate a wider role for industry in the development of codes of conduct and self-regulation, in promoting financial education and public awareness, and in jointly undertaking regular reviews of methodologies and algorithms and developing robust data standards and best practices in data governance and management.

Policy makers and regulators should collaborate with relevant public, private and international stakeholders to review the adequacy and appropriateness of their respective domestic laws and regulations around data and reform them where needed. In undertaking reforms, the following considerations are relevant:

- Reforms should be undertaken using a proactive, holistic and systemic approach. Instead of responding to past challenges, it should be as forward-looking as possible based on an adequate analysis of the technology and industry landscape and trends, as well as scenarios. The reform process should cover the various laws, regulations, institutions and practices that make up the ecosystem governing the generation, collection, storage, sharing and use of data, and create a clear, consistent and effective new framework. The design of laws and regulations governing data should also be informed by the cultural and social values prevalent in the jurisdiction on personal data.

- Policy makers and regulators should adopt a principles- and risk-based approach that is technologically agnostic and avoids being unduly prescriptive. To be successful, this approach will depend on informed expertise to interpret principles for relevant and effective implementation. The industry, which should involve all relevant stakeholders including incumbent financial institutions and new technology-based market players together with major organizations representing users of financial services, can develop codes of conduct based on the principles and undertake self-regulation, in coordination with supervisory authorities and under the oversight of regulators.

- Regulation should be flexible and proportionate, ensuring that restrictions are limited to those that are necessary and allowing the market and consumers to derive the most benefit from the collection, sharing and use of data. This involves, for example, distinguishing sensitive from non-sensitive data based on type, source and use, and differentiating among different levels of consent requirements based on the sensitivity of data and their use. Regulations should also consider multiple bases for processing personal data, such as legitimate interest.

- Regulations should focus on preventing and imposing punishments on the misuse of data rather than the assembly and use of data, as long as the collection and use meet the agreed principles. Preventive and punitive measures should be calibrated in proportion to the potential harm to data subjects and their family that can be caused by such misuse.

- Policy makers and regulators should ensure a level-playing field among market participants that can ensure consistent regulation and supervision for the protection of consumers and the financial system. However, in order for regulation to allow continued innovation, regulators should shift from entity-based to activity-based regulation. Financial services providers should have equal access to data.

Cross-Border Data Flows

APEC economies should identify concerns that are currently being addressed or planned to be addressed through data localization, such as data privacy protection, maintaining cyber resilience, enabling access to data for law enforcement purposes, and the development of domestic technology and data-driven industries. They should evaluate whether these objectives can be better met through other measures that can go hand-in-hand with wider cross-border sharing of data, given the latter's critical importance to the realization of regional economic integration, the empowerment of MSMEs and sustained innovation and economic growth.

APEC should complete a gap analysis between the CBPR/APEC Privacy Framework and the GDPR and identify steps to achieve inter-operability between the two frameworks. Parallel to this effort, APEC should provide a platform for member economies who agree to undertake thorough gap analyses between their domestic privacy regimes and the CBPR/APEC Privacy Framework. The gap analyses should aim to identify the areas where domestic regimes are comparable to the CBPR/APEC Privacy Framework as well as the areas where gaps exist, and develop measures to address those gaps to enable recognition that CBPR-certified organizations meet domestic legal standards. These gap analyses should involve collaboration among relevant government agencies and regulators, the private sector and international organizations, including the APFF.

APEC should promote broader industry participation in the CBPR by introducing mechanisms that would allow MSMEs to participate (e.g., a lower-cost version of the CBPR) and creating a globally recognizable certification mark to attract more companies to apply for certification as CBPR-compliant.

APEC should develop a long-term strategy for strengthening data security in the region by convening a series of conferences and discussions among relevant experts from the public and private sectors, global standard setters such as the ICCR and international and academic institutions toward this end. This strategy could include, among others, the adoption of baseline agreed standards on cybersecurity, the development of comprehensive guidelines on data security and business continuity that balances innovation and safety, expansion of intelligence-sharing on cybercrime, development of innovative programs for promoting security in the payments and lending industries especially in encryption and authentication, the use of regulatory sandboxes to develop innovative digital products and services while ensuring that appropriate protections and safeguards are in place, the design of incentives for company directors to treat cyber resilience and privacy as priority issues, and leveraging existing resources and international expertise for capacity building of regulators.

Individual jurisdictions should review cyber resilience legislation involving all major relevant stakeholders in the public and private sectors and introduce reforms where needed. The industry should complement the legislation with a set of industry best practices developed at the regional level.

Governments should reform the Mutual Legal Assistance Treaty (MLAT) system to streamline the process of providing cross-border access to law enforcement officials to digital information for criminal investigation and prosecution purposes. Various reform proposals that have been put forward should be considered, particularly the use of online forms. As the process of reforming the MLAT system may take several years, member economies should also consider undertaking and expanding international agreements for law enforcement authorities to have access to relevant data in each other's jurisdictions. Governments should develop partnerships where possible within existing laws to allow for greater coordination and cooperation between the public and private sector.

Member economies should develop domestic data-driven industries by developing a holistic set of enabling policies and measures, including educational measures and the expansion of digital infrastructure, to help entrepreneurs and workers benefit from digital trade opportunities, and ensuring that they have access to the data and technologies they need, based on the APEC Blueprint for Action on Electronic Commerce and the APEC Best Practices to Create Jobs and Increase Competitiveness.

APEC economies should develop regional public-private sector platforms to enable policies and regulations that can facilitate cross-border flows of financial services and data through the promotion of existing and development of new minimum benchmarks. Key objectives that could be pursued through these platforms are: (a) a framework of shared accountability and responsibility that can guide financial service industry players that are rapidly adopting tech-based models; (b) pool scarce human resources who can support policy and regulatory awareness and development, such as in translating principles-based regulations into implementable and practical requirements; (c) the design of principles-based legislation and regulations; (d) establishment of a clear consumer recourse process to support the uses of data analytics and intelligence; and (d) coordination among regulators and industry in the region in developing industry codes and standards to complement and support legal and regulatory frameworks.

Introduce regulatory sandboxes that both incumbents and new entrants can utilize and that are coordinated across jurisdictions wherever there is potential to facilitate the development of innovative financial services. APEC should also support and build on existing MOUs; to look at where the gaps and roadblocks would be for fintech firms in either market to gain approvals and be able to enter the other after having met necessary requirements during sandbox experimentation; and to look to broaden the MOUs out to include multiple economies.

ADVISORY GROUP
MEETING PAPER 3-B

An APEC Roadmap for a New Financial Services Data Ecosystem

1. INTRODUCTION

Today's data revolution has tremendous potential to make financial services more inclusive and efficient. This revolution has been driven by consumers benefiting from sharing their data, companies using data to improve and offer new services and increase their efficiency, and regulators promoting competition and better access to finance. It is characterized by the exploding volume of data and variety of their sources, the increasing velocity with which data are generated, the expanding capacity to store and use data, and organizations' growing demand for data to improve and build new products, services and processes and transform business models.

Data play a central role in financial services, enabling lenders and insurers to make risk-based decisions based on customer information. The explosion of data has already enabled millions to gain access to finance since the beginning of this decade[1] and is further opening up new opportunities to make financial services more inclusive and efficient. For example, insurers are using social media data and analytics to provide faster and more affordable services and expand the scope of their services, for example by providing proactive health advice to clients. Data on farmers are being used by banks to make faster risk-based lending decisions to the farm sector. Predictive analysis of data is reducing risk for lenders, enabling them to offer more loans and investment advice to small businesses and individuals, including those previously underserved such as women and young people.

Various technologies are enabling much larger volumes of data to be more rapidly captured, stored, shared, processed and used. These include artificial intelligence, distributed ledger technology, machine learning, cloud computing, QR code technology, biometrics and data mining among others. By facilitating analysis of large amounts of data, reducing costs and providing tools to enhance customer experience and risk control, they are enabling new players to enter and expand operations in payments, consumer lending, supply chain finance and wealth management.

There is, of course, the other side of the coin, as the same technologies can also be misused. Identity theft, fraudulent use of personal information and harassment are examples of outcomes resulting from misuse. Every day, personal information is being collected through various channels ranging from transactions, sensors, public web and social media to audio and video, machine logs and business apps among others, even as incidences of data breaches continue to increase.

The data revolution is also reshaping the data industry by giving rise to a new type of firm that gathers, processes and analyzes data for commercial purposes. Thousands of such firms in emerging markets are now operating in an unregulated or very lightly regulated space, generating concerns about privacy and consumer protection, on one hand, and these firms' exposure to legal risk due to the lack of regulatory clarity, on the other. Formulating new regulatory frameworks that are clear and balanced is important to address risks, promote this new industry's positive contributions to society and continued innovation.

The realities of business in the 21st century and APEC's goal of free and open trade and investment, with micro-, small and medium enterprises (MSMEs) becoming increasingly involved in digital and global supply chains and operating across jurisdictions, underscore the need to develop legal and regulatory regimes that can facilitate cross-border data flows, as well as address the ethical dimension of the collection, sharing and use of data. This aspiration clashes with most current legal and regulatory frameworks around the governance of data in the region, which are still predicated on largely domestic considerations.

---

[1] The World Bank reported that 1.2 billion adults have obtained an account since 2011, including 515 million since 2014, mostly with the help of mobile phones and digital payments. World Bank, *Global Findex Database 2017* [https://globalfindex.worldbank.org/]

Technological innovations have been driving policy and regulatory reforms, alongside exogenous events such as major data breaches that have pushed data security and privacy to the forefront of regulators' concerns. Most of these responses so far have been reactive rather than proactive, but more and more governments and regulators are now seeing the need for a more proactive approach.

Since a few years ago, governments in developed economies started moving to open data access, beginning with their own, and many in the private sector have followed in their wake. The driving forces behind this push by governments to make more data available include the desire to use it to foster more competition, as well as the growing pressure from the technology sector (including fintech firms), from non-governmental organizations and from multilateral institutions.

However, even as government support for more open data access grows, privacy and security concerns have served to temper the pace of this response. Various regulations were introduced in many developed economies in response to several major incidents that have occurred over the past decade.[2] In emerging markets where growth in consumer data-driven financial services has been rapid, new service providers today find themselves faced with very strict civil, criminal and cybersecurity laws and a lack of regulatory framework specific to their industry that create an uncertain business environment. In these markets, firms are constrained from sharing more data and so have to set up their own internal ecosystems.

There is a growing realization around the world that data is important in meeting the needs of businesses and consumers in today's digital economy. Several jurisdictions are currently undertaking efforts to develop next generation legal and regulatory frameworks around data.[3] However, while most of these responses reflect a trend toward increased access to data, efforts are uncoordinated and the continued existence of data silos, varying approaches to data security and privacy, unresolved issues around competition and level-playing field, and the lack of capacity of many jurisdictions to implement new rules or comply with those extraterritorially impacting them are all likely to lead to continued inefficiencies and increased frictions.

Ensuring progress in harnessing the potential of technology and data to achieve greater financial inclusion and efficiency calls for efforts within APEC to develop a shared vision of a future data ecosystem and to collaborate in achieving this. It requires clearer awareness that laws and regulations taken in response to concerns, such as those about data privacy and security, have consequences on the costs of financial services. Toward this end, key stakeholders from the private and public sectors and multilateral and academic institutions, using the Asia-Pacific Financial Forum (APFF) under the leadership of the APEC Business Advisory Council (ABAC) as a platform, collaborated to undertake a series of conference calls and a conference in Singapore to create this Roadmap. [*See Appendices A and B for the list of participants and speakers and the conference program.*]

This Roadmap identifies critical building blocks of an enabling data ecosystem for the region and outlines concrete initiatives and actions to put these building blocks in place over a reasonable time frame. It provides a tool for promoting consistency of laws, policies and regulations in APEC economies with existing internationally agreed principles, frameworks and good practices, and identifies areas where new minimum benchmarks need to be developed in order to achieve regional consistency. It also points out key considerations and the way forward for individual jurisdictions to undertake reforms and for regional cooperation to be harnessed for the purpose of promoting expanded collection, sharing and use of data within and across jurisdictions leading to greater

[2] These include the 2008 Global Financial Crisis that resulted in host of legal and regulatory initiativs, the 2013 NSA-Wikileaks and the 2017 Equifax breach that created a furor over data security and the 2018 Facebook incident that made data privacy an important policy issue.

[3] Examples are AnaCredit, the General Data Protection Regulation (GDPR) and the Payment Services Directive (PSD2) in the EU, the principles for Consumer-Authorized Financial Data Sharing and Aggregation in the USA and the New Payments Platform (NPP) in Australia. Canada, Japan, Korea, Mexico, Singapore and the USA are participating in the APEC Cross-Border Privacy Rules (CBPR).

inclusiveness and efficiency of financial services in the region.

2. GENERAL DATA REGULATION

2.1. Core Principles of Data Protection

There is general agreement across jurisdictions on the core principles of data protection. The "Basic Principles of National Application" of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were adopted in 1980, continue to be considered as the fundamental basis for the development of legislation and regulations around data around the world. Subsequent initiatives such as the APEC Privacy Framework[4] and the proposed update to the OECD Guidelines by the Oxford Internet Institute [5] adopted modified versions but are fundamentally consistent with the principles. The sections on data protection and privacy in each of the financial subsector chapters of the World Bank Group's *Good Practices for Financial Consumer Protection*[6] also provide practical and detailed guidance for implementation.

It is widely acknowledged that the Principles are meant to serve as guide for legislation and policies whose details will need to be fitted to the conditions of each jurisdiction. Given the diversity among jurisdictions, especially in the Asia-Pacific region with its economies' varying historical experiences, cultures and levels of development, data protection laws may differ significantly in their details. However, it is important to achieve some level of consistency to allow for inter-operability among data protection regimes that would enable cross-border transactions, including trade, investment and financing activities.

Proposed action:

- In developing personal data protection laws and regulations that meet the specific needs of their respective jurisdictions, economies should strive for consistency with the APEC Privacy Framework, the Basic Principles under the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* and the World Bank's *Good Practices for Financial Consumer Protection.*

2.2 Consistency among Domestic Laws and Regulations

Data protection laws have been evolving across the world, where as of today more than a hundred jurisdictions have enacted such legal frameworks, of which data privacy forms a part. There are also, however, specific laws on data privacy and cybersecurity.[7] In various jurisdictions, numerous laws at different levels of government (e.g., federal and provincial) impact data privacy.[8] In addition, there are overlaps of responsibility among different regulators (e.g., data protection regulator and consumer protection regulator), which are not always well-coordinated. As a result, companies and organizations have to simultaneously deal with a complex set of multiple rules at different levels governing data within the same jurisdiction.

---

[4] https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

[5] This version sought to inject the context of 21st-century technologies and big data in considerations to balance privacy and the free flow of information to focus on data use rather than data collection. Oxford Internet Institute, Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines (2014) [https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf].

[6] http://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection.

[7] Examples are Hong Kong's Personal Data Privacy Ordinance and China's new Cybersecurity Law.

[8] An example is Australia, where the Telecommunications Act of 1997 (federal), the National Health Act of 1953 (federal), the Health Records and Information Privacy Act of 2002 (NSW), the Health Records Act of 2001 (Victoria) and the Workplace Surveillance Act of 2005 (NSW) all impact data privacy protection for specific types of data and activities.

Another key issue is inconsistency across laws, policies and regulations that lead to perceived conflicting regulatory expectations. Examples are promoting open banking, data analytics and data sharing on one hand while regulatory responsibility sharing models among participants remain unclear on the other; imposing data localization for domestic security purposes on one hand while promoting cross-border electronic commerce and more efficient electronic payments on the other; and AML/CFT requirements on trade finance that need cross-ecosystem data pooling to be efficient on one hand, and data privacy, consent and confidentiality requirements on the other.

Proposed action:

- Economies should promote consistency among the variety of domestic laws, policies and regulations within their respective jurisdictions impacting the generation, collection, storage, sharing and use of data across central-level ministries and agencies and different levels of government, by reviewing these laws, policies and regulations in collaboration with the financial industry, enterprises and consumers, and undertake changes where needed to reinforce agreed objectives. Reforms should be undertaken using a proactive, holistic and systematic approach. Instead of responding to past challenges, it should be as forward-looking as possible based on an adequate analysis of the technology and industry landscape and trends, as well as scenarios.

2.3. Expanding the Collection and Sharing of Data

2.3.1. Full-file and comprehensive credit information systems

With its rapidly growing availability, there is great potential for data, and particularly credit data, to be harnessed using new technologies, to promote financial inclusion and specifically to address MSMEs' lack of access to finance. Various studies confirm that the use of more data about individual consumers and borrowers in creating credit scores (for example by including not just negative credit data, but also positive credit data) make financial services more inclusive and increase benefits to underserved communities such as ethnic minorities and women, as well as help lenders mitigate risks and increase lending to the private sector.[9]

For example, credit scores used in underwriting loans rely in many cases on traditional data, which capture mostly consumers' transactions with financial institutions. [10] However, people without bank accounts or with thin credit histories, usually referred to as *credit invisibles*, cannot obtain credit scores using only traditional data, and thus are forced to rely on high-priced short-term loans. A recent study by Brookings and the Policy and Economic Research Council (PERC) found that including alternative or non-traditional data such as utilities payments could potentially reduce the

[9] See for example Michael A. Turner, Patrick D. Walker, Sukanya Chaudhuri, Joseph Duncan and Robin Varghese, Credit Impacts of More Comprehensive Credit Reporting in Australia and New Zealand (PERC, May 2012) [http://www.perc.net/wp-content/uploads/2013/09/PERC-Report-Final.pdf]. See also Turner, Walker, Varghese and Chaudhuri, *The Credit Impacts on Low-Income Americans from Reporting Moderately Late Utility Payments* (PERC, August 2012) [http://www.perc.net/wp-content/uploads/2013/09/ADI_ML_Impacts.pdf].

[10] A reference to the types of data used in lending decisions would be useful in analyzing this matter: traditional vs. alternative data and structured vs. unstructured data.

- ***Traditional data*** as used in credit scoring are data on a consumer's credit history which may include credit card transactions, loan payments and additional debts, how well they pay their individual credit accounts and data on liens and judgments.
- ***Alternative*** or ***non-traditional data*** are data that go beyond individual consumers' traditional credit activities, which may include their payments of rent, telephone bills, utility bills, insurance premiums and child care payments, among others. Alternative data may be structured or unstructured data.
- ***Structured data*** are traditional and alternative data that are contained in relational databases and spreadsheets, and so can be readily used to create credit scores using proven analytical methodologies. Credit scores derived from them have a high level of accuracy, and can be dealt with through existing redress mechanisms whenever a consumer wishes to contest erroneous or inaccurate data.
- ***Unstructured data*** are a type of alternative data that are derived from social media and other online sources, which are also called Big Data. Unlike structured data, they cannot be fitted into relational databases.

population of credit invisibles in the USA from 60 million to only 5 million people.[11]

The development of a full-file (based on both positive and negative credit data) and comprehensive (using both traditional and alternative data) credit information system will require mechanisms for collecting a wide range of data on individuals and businesses from creditors, non-financial creditors, other private databases, public records agencies and any other relevant source of data within the jurisdiction, as well as operating credit reporting service providers (CRSPs), which include credit bureaus and credit registries.

In many emerging markets, such efforts face a number of practical challenges, such as the lack of unique identifiers for differentiating data subjects at reasonable cost, poor quality of data and the limited digital footprint of MSME transactions, among others. Legal challenges, such as restrictive models of consent for personal data, also limit the practical utility of such efforts. Measures economies can take to meet these challenges include:

- Introduction of unique identifiers, such as passports and identity documents for individuals in conjunction with central ID databases to enable verification, and company or legal entities' registration numbers for enterprises or the adoption of the Global Legal Entity Identifier (LEI);
- Enabling digital authentication via the development of a digital identity system to remove the need for in-person authentication of individuals or documents, as digital identities will increasingly become a core enabler of the digital economy, facilitating seamless cross-border transactions and trade;
- Promoting automation of data collection, processing and sharing;
- Developing and promoting access to an open data system for MSME data that captures publicly available corporate and financial data;
- Providing guidance on adoption and use of alternative data, including cases when the use of structured and unstructured data may be appropriate;
- Promoting open data platforms for CRSPs to interface with other data repositories such as court records, company registries, collateral registries and other sources of digitalized information;
- Promoting effective and comprehensive sharing of consumer and commercial data by all relevant data providers and sources with authorized entities based on principles such as legitimate use and/or practical consent mechanisms;
- Ensuring MSME data are collected by CRSPs by reducing or eliminating minimum reporting thresholds for reporting creditor and debtors to CRSPs;
- Encouraging different types of CRSPs – commercial credit information companies and consumer credit bureaus – to collaborate, and to the extent permitted by law, share data among themselves that might be useful to each other and to their respective users, and eventually jointly develop certain credit reporting products (e.g.; and
- Assessing the feasibility of establishing a public credit registry or databank where there is inadequate information sharing within the economy.

To facilitate the future development of a regional credit information network, APEC member economies should strive for regional consistency in developing domestic credit information systems. Among the steps they can consider are the following:

- Improving the comparability and consistency of MSME credit data through collaboration with relevant international standard setting bodies and organizations, such as the World Bank's International Committee for Credit Reporting (ICCR);

[11] PERC and The Brookings Institution, *Give Credit Where Credit is Due: Increasing Access to Affordable Mainstream Credit Using Alternative Data*, 2006 [https://www.brookings.edu/research/give-credit-where-credit-is-due-increasing-access-to-affordable-mainstream-credit-using-alternative-data/]. See also Testimony of Dr. Michael A. Turner, President and CEO, Policy and Economic Research Council Before the House Subcommittee on Financial Institutions and Consumer Credit, Financial Services Committee, Examining Legislative Proposals to Address Consumer Access and Mainstream Banking Issues," 27 September 2016 [https://financialservices.house.gov/uploadedfiles/hhrg-114-ba15-wstate-mturner-20160927.pdf].

- Agreeing on a core set of variables to be shared across borders on MSMEs covering both financial data and credit performance aspects; and
- Promoting the adoption of the Global Legal Entity Identifier,[12] to facilitate information on financial transaction participants, support higher quality and accuracy of financial data and help prevent market abuse and financial fraud.

A well-designed legal and regulatory framework that lays down general principles; clearly defines the roles, rights and responsibilities of data providers and sources, service providers, data users and data subjects; and provides effective oversight is key to having a sound, efficient and effective credit information system. The World Bank's *General Principles for Credit Reporting*[13] can serve as a reference for economies in developing or improving their frameworks.

Proposed action:

- Economies should foster a credit information system that is both full-file (based on both positive and negative credit data) and comprehensive (using both traditional and alternative data), by taking steps to improve the availability and accuracy of information and expand the sharing of credit information from various sources, including public data sources, while avoiding restrictive consent models. They should collaborate to promote regional consistency of their domestic systems and support future cross-border sharing of credit information. They should also review their legal and regulatory frameworks for credit reporting and undertake improvements where needed, referencing the World Bank's *General Principles for Credit Reporting* as appropriate.

2.3.2. Uses of unstructured data (Big Data) and industry regulation

Unstructured data (also commonly known as Big Data), which are huge data sets that can only be interpreted and/or analysed by computers, have exploded in volume in recent years, and are increasingly being used in lending decisions. Technologies like artificial intelligence and machine learning have tremendous potential to expand lending to underserved groups and advance financial inclusion. Barriers still exist currently though, as such data from social media, sensors in devices, business apps or machine logs cannot yet be used for credit scoring with the same level of confidence as structured data, and there are no standard mechanisms to protect data subjects against the use of inaccurate or erroneous data or to fairly and transparently notify them that their data are in fact being utilized and incorporated into credit decisions.

The use of big data could also lead to inadvertent re-identification of personal data. Given the unstructured nature of such data, traditional consent models may not be effective in protecting individuals' personal data.

As technology evolves and new use cases and business models emerge, however, it would be reasonable to expect that in coming years unstructured data will play an ever increasing role in financial services, including risk-based lending. It is therefore important to develop forward-looking regulatory, governance and consent approaches that can allow continued innovation in this space.

Within the Asia-Pacific region, advanced markets typically have an existing comprehensive personal data protection law and a special regulatory authority. Some of the more sophisticated emerging markets also have similar models, but the awareness level tends to be low and capacity to implement needs improvement. Other less developed and nascent markets have some segmented provisions in various laws as well as sectoral regulations, but no comprehensive personal data protection laws and

[12] The Legal Entity Identifier (LEI) is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. [https://www.gleif.org/en]

[13] World Bank, *General Principles for Credit Reporting* (September 2011) [http://documents.worldbank.org/curated/en/662161468147557554/General-principles-for-credit-reporting]

no general regulator, with low awareness and little willingness to reform.

While the data and analytics industry in some emerging markets has outgrown the conventional credit reporting industry and continues to expand, it remains largely unregulated and now poses increasing risks for consumers, businesses and governments. Challenges that these jurisdictions face in establishing a comprehensive data regime include the political and technical difficulties of developing new laws and setting up new government agencies; the near impossibility of finding a lead agency to champion a new course; mixed and emotional public perceptions about personal data protection; and inadequate knowledge, understanding and willingness of many policy stakeholders.

Continued innovation and development of this industry will require a flexible regulatory regime that is different from that currently being applied to conventional credit reporting entities and ensures a balance between innovation and inclusion on one hand and protection of consumers and financial system integrity on the other. It will need to be comprehensive, covering all stages of the data life cycle and going beyond financial services or the credit life cycle. Regulators shall be looking at their regulated financial service providers' compliance with both credit reporting requirements and general data protection requirements. While sophisticated jurisdictions are mostly in line with these best practices, developing and nascent jurisdictions face major difficulties.

Proposed action:

- Emerging markets should adopt a balanced regulatory approach toward the new data analytics industry that fosters continued innovation and inclusion while also protecting consumers and financial system integrity. They should strive toward developing and/or maintaining a comprehensive and dedicated law or an over-arching regulation on personal data protection that reflects this approach, and establish where needed a general personal data regulator that has capacity to implement and power to enforce personal data protection in parallel with established financial regulators. The data ecosystem should also include an independent industry association and practice codes of conduct; efficient and low-cost complaint, correction and dispute resolution mechanisms, particularly out-of-court procedures; rules governing cross-border data cooperation, investigations and data flows; and specific financial sector regulations and guidelines for firms providing financial services. As the largest holder of data in the economy, government should stimulate the growth of the market by making public data available in a convenient manner for pre-approved legitimate business purposes.

2.4. Creating Sound Frameworks for the Collection, Storage, Sharing and Use of Data

2.4.1. Data Protection and Privacy in the Digital Age

Some of the region's jurisdictions introduced comprehensive local privacy laws before the Internet age and long before the data revolution. Where this was the case, laws typically contained mostly basic data protection principles based on the OECD Guidelines, enforcement mechanisms were mild, privacy commissioners did not have adequate powers, and there was no mandatory requirement for data protection officers (DPOs), as privacy was then a new concept not conceived in common law systems. As technological changes impacted privacy, these laws were updated incrementally through guidance notes, amendments and patches.

Many other jurisdictions, however, introduced comprehensive privacy laws more recently, often in response to major incidents of data breaches. These tended to have more stringent requirements and steeper sanctions, in cases including fines and imprisonment for unauthorized processing, access and disclosure of personal data. DPOs have stringent ongoing roles and responsibilities that entail serious personal liability. The trend toward stricter privacy laws has continued with the coming into force of the GDPR, which has extraterritorial reach and steep penalties for violations. The introduction of the GDPR and privacy frameworks across the region has also added new compliance costs for financial institutions and businesses, impacting their efficiency.

The flurry of privacy legislations introduced in recent years has resulted in a more diverse privacy

landscape across the globe and the region that reflects the diversity of cultures, traditions and local views on personal data. Some jurisdictions treat privacy as a constitutional right, with all other laws expected to accommodate this right. Others consider personal data as property (similar to money), with unauthorized access equated to theft and with serious sanctions imposed. There are also jurisdictions that view an individual's right to personal data as a right created by legislation and protected by principles.

The trend toward more new and stricter personal data protection regimes and growing divergence across jurisdictions provides a complex backdrop for efforts to develop personal data protection regimes that can allow economies to reap the benefits of the data revolution. Legislators and regulators are facing the challenge not only of defining the privacy rights of individuals in the context of the digital age and its new opportunities, but also the challenge of defining and shaping privacy in the context of how it is viewed in their respective societies, such as whether it is merely a right accorded by legislation that should be balanced with public interest, or whether it is sancrosanct and needs to be protected at all costs.

An important consideration is how to distinguish between personal data that need stronger protection and the ones that can be more readily shared. Personal data are sourced from both public (e.g., voter registration; deeds, licenses, bankruptcies) and private (e.g., lender records, customer lists, surveys) records. Some data contain personally identifiable information (PII), while others do not, but there are also multiple data elements that can be combined with other data to identify a data subject. The APEC Privacy Framework defines personal information as any information about an identified or identifiable individual, and so provides a broader interpretation of PII.

In addition to this challenge, policy makers and regulators are grappling with the implications of new technologies such as Internet of Things, intelligent personal assistants, health monitors, drones and satellites, as well as new use cases and business models. Their continued rapid evolution create concerns about the continued relevance and effectiveness of existing legal and regulatory frameworks in serving the interests of individuals and organizations. This includes the implications of the increasingly large volume of data being generated, collected, stored, shared and used, new ways of collecting data (including those that individuals are not conscious of), new ways of transmitting data, new ways of storing data (such as through a decentralized block chain) and the changing concept of data (including the trend to view data increasingly as an asset), as well as the challenge of keeping data secure.

The new data landscape in the digital age necessitates a review of the adequacy and appropriateness of existing laws and regulations around data, particularly those that were introduced under conditions much different from those of today, and those that constitute an uncoordinated patchwork of piece-meal responses to a variety of major incidents at different times in the past. Providing an inclusive and efficient legal, policy, regulatory and institutional data ecosystem will require the involvement of a broader set of public, private and international stakeholders who look at the ecosystem from different angles, including the social, cultural, economic, technological, international and security angles, and a proactive, holistic and system approach (instead of an item-by-item approach) to policy reform. This, however, also requires a deeper understanding of the changing data technology and industry landscape by policy makers and regulators.

With the expansion of the volume of data that can be used, it is important to ensure that regulations are flexible and proportionate to allow its positive impact on inclusion, efficiency and innovation to be realized. All data should not be regulated in the same way, because they are different with respect to type (e.g., sensitive health data should be treated differently from marketing or geographical data), source (e.g., private vs. public record), and use (e.g., lending decisions vs. lists to send coupons in the mail). General frameworks should underscore that the details of data protection regulations and how they are applied to particular types of data need to take account of important differences in the types, uses and sources of data. Data governance should be built upon a combination of general principles, company policies and agreements, industry guidelines and standards and government regulations.

The burden of maintaining a sound data ecosystem should not be borne by regulators alone. Industry, which can deploy many subject matter experts, can play an important role through the development of codes of conduct, certification schemes and self-regulation. There is also a role for financial education and public awareness in helping consumers understand the risks, make good financial decisions, put pressure on market players to adhere to ethical standards, and reduce the strain on the system caused by consumers being harmed by misuse of data.

2.4.2. Consumer Consent and Use of Personal Data

The tension between the rights of individuals and society is a theme that runs through the data industry. On one hand, the individual consumer needs to be protected from misuse of his personal information. On the other, personal information of consumers can be used to benefit not only the consumers themselves, but society as well. The industry is expected to protect personal data from misuse, and regulators have the task of ensuring compliance with relevant laws and regulations. The consent requirement is the tool consumers have to influence how their personal data are used.

The balance between consumer consent and data availability is a range of possibilities, and how the consent requirement is defined by laws and regulations determines where that balance lies within a particular jurisdiction. Values and preferences differ across societies and generations. Privacy is valued more highly in some societies than others. In some economies, more people are willing to trade personal information for commercial benefits, and in many economies, more members of the younger generation tend to do so as well. Personal information is also defined differently in different jurisdictions, as exemplified by differences between the EU GDPR and US Sectoral Law.[14]

Improper uses of data pose different levels of risk to consumers depending on what those uses are. Currently, financial institutions use data for a large variety of purposes, including consumer, commercial and portfolio risk management, credit scoring, collection, processing payment, deposit and purchase transactions, application processing, branch or site location, data hygiene (keeping data up-to-date), partnership and prospect marketing, customer up-sale and cross-sale, product development, identity management and authentication, customer relationship management, fraud detection, customer due diligence (including KYC/AML/CTF), employment, and customer and employee safety, among others.

Consumer consent is not the sole basis for processing and using consumer data, but one of several. Under the GDPR, for example, processing consumer data is also necessary for contracts, compliance with legal obligations, protecting vital interests of individuals (e.g., protecting someone's life), performing a public task with a clear basis in law, and protecting the legitimate interests of a person. Under US Sectoral Laws, permissible purposes and allowable uses of data have been itemized. Laws forbid the use of data for any other purpose; govern collection practices and consumer notification processes; set forth consumer consent standards based upon the sensitivity of the data; and govern the data as they pass from one entity to another.

Consent involves a continuum of consumer permissions. The GDPR describes clear and unambiguous consent as ranging from informed consent to express consent, depending on sensitivity of data and their use. Express consent requires a consumer to take action such as by checking a box. Affirmative consent may include a pre-checked box. In the case of informed consent, the consumer is provided a clear notice of collection and use practices and consent is assumed unless the consumer objects or opts out.

---

[14] The GDPR defines personal data as"any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."US Sectoral Law on the other hand defines it as "a combination of any information that identifies an individual with that individual's sensitive and non-public financial, health or other data or attribute, such as a combination of the individual's name, address, or phone number with the individual's social security number or other government issued number, financial account number, date of birth, address, biometric data, mother's maiden name, or other personally identifiable information."

Key to resolving the tension between information sharing and consumer data protection is finding the point where the economic and social benefits derived from robust information sharing can be attained without the need to sacrifice meaningful data protections and the rights of data subjects. This would require efforts to design the details of consent and data protection in a way that can both promote data sharing and protect the rights of data subjects to access their own data, control access to their data by other parties, and contest inaccuracies. Through proper design and a good understanding of the local culture and market, robust data sharing and meaningful data protection can both be achieved.

However, many APEC-economies' laws utilize consent as the main method for ensuring transparency over the use and disclosure of personal data. Such consent models have many limitations, chief among which is that privacy notices to which the consent is tied frequently become long and legalistic, thus reducing the transparency such consent models were intended to promote. Recognizing the limitations of the consent model, the GDPR allows for "legitimate interest" as a basis for processing personal data in addition to consent. The advantage of this approach is that it balances the interests of organizations with those of individuals, recognizes that organizations are in the best position of assessing the risk and impact of personal data processing, and organizations can implement mitigating measures when processing personal data. Once mitigating measures are in place, then the organization may have considerable freedom to process personal data, possibly in innovative ways that cannot be envisaged when laws are drafted.

2.4.3. Use of Data and Derived Data: Rights and Responsibilities

Legal and regulatory frameworks around data are shaped by how societies view the rights and responsibilities of data providers and sources, service providers, data users and data subjects, and there are differences in how jurisdictions approach this matter. An important example is how the term "ownership of data" is interpreted. The EU GDPR explicitly states that data is owned by the data subject and thus cannot be processed without the data subject's consent. This derives from the view that everyone has the right to the protection of personal data.

In the USA, the concept of data ownership is not clearly defined, with the collector of data being treated as the owner of the data in practice, as personal data are widely collected, analyzed and traded. There are sector-based laws that focus on consumer protection, which are calibrated to the sensitivity of the data, but there is no uniform scheme for the protection of personal data. Under US law, customer lists collected by organizations are treated as trade secrets owned by whoever assembles and maintains the list. Unlawful appropriation of such property is subject to legal sanctions. For example, when a person visits a web site, any information gleaned by the web service provider, such as payment method, recipient information, delivery address, location of the person making an order are included in the information that the web host could protect as its own property.

Database protections in the EU, the UK and the USA also imply that entities aggregating and using data have rights to the data. The EU Database Directive (EU Directive 96/9/EC) adopted by the European Commission in 1996 states as its objective "to afford an appropriate and uniform level of protection of databases as a means to secure the remuneration of the maker of the database," although it makes a reference to Directive 95/46/EC governing the processing and circulation of personal data. UK law clearly identifies the compiler as owner of data in stating that a "property right (database right) subsists, in accordance with this part, in a database if there has been substantial investment in obtaining, verifying or presenting the contents of a database." The US Copyrights Act provides protection to compilations so long as there is copyrightable authorship in their selection or arrangement.[15]

The concept of ownership is normally associated with the right to exclude others from a piece of property, including intellectual property. Such properties are typically protected by physical barriers

[15] Source: International Association of Privacy Professionals. Downloaded at: https://iapp.org/news/a/2012-12-01-the-ownership-and-exploitation-of-personal-identity-in-the-new/

or by force of law. In this context, it is unclear how a person can exclude others from collecting, distributing and using their personally identifiable information (PII) and impossible to control how other people use that information without placing undue restrictions on basic freedoms, particularly of the entity that aggregates and uses the information

The above considerations lead to the conclusion that the compiler is effectively the owner of the data (in the sense of being able to exclude others from exercising control) and data subjects have limited ability to exclude firms from collecting, distributing and using their data. The compiler has wide latitude to use personally identifiable information (PII) for purposes of making profit. It is difficult to legally distinguish between an author selling a book containing PII for profit, which is not unusual, and an Internet firm doing similar things with most customer information.

With respect to derived data, which are being collected at a rapidly accelerating pace across all spheres, it can also be argued strongly that the compiler is the owner and can neither be prevented by data subjects from collecting, distributing nor using derived data.

The key issue, however, is not the ownership, but the use of the data, or more specifically the potential misuses of data by the compiler and third parties to whom data are sold or are shared. In practical terms, what is important is regulation against misuse of data. In US law, the approach to PII is similar to the Dangerous Instrumentality Doctrine[16] where ownership must be strictly regulated to avoid harm and unlawful exploitation. Regulations are calibrated in proportion to the ability to cause harm to data subjects and/or their family. The US and EU GDPR are in agreement that the assembly of personal data is permitted and encouraged, but are subject to a myriad of personal data protection laws. The rights of data subjects are spelled out in the OECD Fair Information Principles and also commonly specified, for example, in the general prohibition against the use of data relating to race, ethnicity, religion and medical conditions in decisions within the financial services sector.

2.4.4. Ensuring a level playing field

The entry of new companies leveraging technology and data into financial services, including payments, consumer and commercial lending, wealth management and supply chain finance, has opened up the question of how regulators can ensure a level-playing field. Banks, which in the region hold the bulk of financial resources and customer data, are subject to a myriad of regulations that have impact on compliance and operating costs as well as legal and regulatory risks. In most jurisdictions, there is no well-developed regulatory framework for fintech firms.

Light-touch regulations applied to fintech start-ups have allowed innovation to flourish in various markets. However, as risks to consumers and the financial system become significant, regulators will need to step in. To ensure consistent regulation and supervision of both banks and fintech companies to protect consumers and financial system stability and integrity, while encouraging continued innovation (which will be difficult if non-deposit taking fintech companies will be regulated in the same way as deposit-taking institutions), regulators will need to shift their approach from entity-based to activity-based regulation, which will also provide a level-playing field that can benefit consumers and ensure healthy competition in financial services.

One of the major issues is what type of financial data should be shared between banks and fintech companies, which can affect liabilities of each party as well as change competitive dynamics and the extent of disintermediation for banks. Different approaches currently exist in various jurisdictions. The EU's Payment Services Directive 2 (PSD2) required banks to share transaction and account data of customers who have given their consent with EU-licensed third-party service providers. In the USA, the Consumer Financial Protection Bureau (CFPB) published in October 2017 new principles for consumer-authorized data sharing and aggregation regarding individual consumers. While

[16] The Dangerous Instrumentality Doctrine applied in Florida is a common law concept that says that the owner of a tool that is inherently dangerous is liable for any injuries that result from the operation of the tool.

opening up access to data, banks retain more control over API access compared to PSD2 in Europe. An associated issue is on the control of APIs, which can impact industry and cross-border technology standardization and the cybersecurity standards on both banks and fintech firms. Both of the above examples highlight the range and depth of topics that would be involved, and the need for capacity, readiness and consultation by economies seeking to promote innovation through more financial data sharing between banks and fintech firms.

Many fintech companies in smaller Asian markets are data users and not data generators. However, there are also large fintech companies in Asia that have become repositories of large amounts of consumer data and have established monopolies or near-monopolies in their respective sectors. To benefit the economy as a whole and promote financial inclusion and efficiency, jurisdictions should move toward the sharing of data among all financial services market participants, consistent with the above proposed action related to full-file and comprehensive credit information system to collect traditional and structured alternative data and make them available to financial service providers under a robust regulatory framework in accordance with the World Bank's *General Principles for Credit Reporting*. Consumers should also be encouraged to be aware of and responsible for their data that are shared, balanced with practical consent mechanisms and principles such as legitimate use.

2.4.5. Ensuring Confidence and Trust in Algorithms

Algorithms have been used in the credit information industry in developed economies for many years, and models have been developed with the use of artificial intelligence (AI) and machine learning (ML). Practices have emerged within the industry to ensure compliance with regulations and the robustness of processes underpinning credit bureaus' operations. These include:

- Looking at global and local regulations and understanding the highest global and local standards;
- Ensuring that processes are well documented;
- Separating model development and validation control; and
- Ensuring the appropriateness of the data governance process, which involves looking at the palatability of data from the legal perspective, the depth of information that can provide enough detail to offer value, consistency, reliability of data, usefulness in predicting human behavior, and complementarity of captured data with those already captured in other data sources.

One key issue is the type of data that can be used for risk-based lending decisions. Within the credit information industry, ensuring confidence and trust in algorithms using AI and ML involves a focus on data quality and a clear hierarchy of data sources according to their predictiveness. Traditional data are at the top of this hierarchy, followed by structured alternative data. Unstructured data pose challenges as current technologies and algorithms do not yet allow their use with the same degree of confidence as structured data.

A second issue is ensuring the robustness of processes underpinning credit scores. ML has been very useful in facilitating the predictive use of data. However, regulators remain cautious regarding the transparency and palatability of data. Transparency presents challenges in the case of commercial service providers where the methodology for scoring are part of the company's intellectual property. A way to deal with this issue has been to allow regulators to look at the process in each company to develop an adequate understanding of how the model is used to calculate scores and provide guidance to the data service provider.

A third issue is ensuring trust in the fairness of outcomes. There is public concern that the use of AI could result in unfair or socially unacceptable outcomes. Various financial institutions have adopted technology such as AI in a way that also allows human intervention, to avoid such issues. Financial regulators and international organizations can play a role by promoting data standards and best practices in data governance and governance organization.

In other areas of finance, such as robo-advisors, regulators are focused on the parameters that determine how algorithms lead to outcomes. Walking a fine line between protecting investors and promoting innovation, regulators are focused on improving transparency to ensure that best

practices are being followed. The major challenge facing the use of algorithms in these other areas is the quality of data (data hygiene) in the financial services sector of many advanced economies, and the current limitations of AI in operating outside closed systems.

2.4.6. Proposed actions:

- In addition to alignment on key principles like transparency, open data and interoperability, APEC should undertake capacity building activities to help relevant policy makers and regulators deepen their understanding of the changing data technology and industry landscape and enhance their readiness to undertake policy reforms. It will also help them to effectively engage with data service providers in ensuring their compliance with laws and regulations and to be able to make good judgments on the soundness, inclusiveness and fairness of their operating models, methodologies and algorithms and provide effective guidance.

- Regulators should collaborate with industry to facilitate a wider role for industry in the development of codes of conduct and self-regulation, in promoting financial education and public awareness, and in jointly undertaking regular reviews of methodologies and algorithms and developing robust data standards and best practices in data governance and management.

- Policy makers and regulators should collaborate with relevant public, private and international stakeholders to review the adequacy and appropriateness of their respective domestic laws and regulations around data and reform them where needed. In undertaking reforms, the following considerations are relevant:

  - Reforms should be undertaken using a proactive, holistic and systemic approach. Instead of responding to past challenges, it should be as forward-looking as possible based on an adequate analysis of the technology and industry landscape and trends, as well as scenarios. The reform process should cover the various laws, regulations, institutions and practices that make up the ecosystem governing the generation, collection, storage, sharing and use of data, and create a clear, consistent and effective new framework. The design of laws and regulations governing data should also be informed by the cultural and social values prevalent in the jurisdiction on personal data.

  - Policy makers and regulators should adopt a principles- and risk-based approach that is technologically agnostic and avoids being unduly prescriptive. To be successful, this approach will depend on informed expertise to interpret principles for relevant and effective implementation. The industry, which should involve all relevant stakeholders including incumbent financial institutions and new technology-based market players together with major organizations representing users of financial services, can develop codes of conduct based on the principles and undertake self-regulation, in coordination with supervisory authorities and under the oversight of regulators.

  - Regulation should be flexible and proportionate, ensuring that restrictions are limited to those that are necessary and allowing the market and consumers to derive the most benefit from the collection, sharing and use of data. This involves, for example, distinguishing sensitive from non-sensitive data based on type, source and use, and differentiating among different levels of consent requirements based on the sensitivity of data and their use. Regulations should also consider multiple bases for processing personal data, such as legitimate interest.

  - Regulations should focus on preventing and imposing punishments on the misuse of data rather than the assembly and use of data as long as the collection and use meet the agreed principles.[17] Preventive and punitive measures should be calibrated in proportion to the

[17] Alignment with OECD principles require organizations also respect the collection limitation principle (irrespective of misuse).
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#pa

potential harm to data subjects and their family that can be caused by such misuse.

- Policy makers and regulators should ensure a level-playing field among market participants that can ensure consistent regulation and supervision for the protection of consumers and the financial system. However, in order for regulation to allow continued innovation, regulators should shift from entity-based to activity-based regulation. Financial services providers should have equal access to data.

3. CROSS-BORDER DATA FLOWS

The cross-border flow of data is an important issue for Asia-Pacific economies, as their continued prosperity depends to a great extent on the growth of trade and investment across the region, which is powered by data. This is especially critical to developing economies, which have much to gain from the integration of MSMEs in global and regional supply chains and have large migrant populations overseas that send back remittances contributing to the growth of the domestic economy. The advent of the digital age has created channels and technologies through which MSMEs can access markets and financing even from the remotest location. How these opportunities can be realized depends to a large extent on the development of a policy ecosystem that will enable the cross-border flow of data.

3.1. Addressing the Concerns behind Data Localization

In recent years, there has been a growing trend toward data localization, which requires that data on residents be collected, processed and/or stored inside a specific jurisdiction. Data localization takes on different forms. Some jurisdictions prohibit the transfer of data abroad. Others allow the transfer of data outside their jurisdictions, but require copies to be maintained domestically. Some others allow global transfers but mandate prior consent by individuals or government. Data localization has been driven by a variety of concerns, including data privacy protection, cyber resilience, law enforcement and regulatory access to data held outside of their jurisdictions, and promoting the growth of local infrastructure and domestic firms by shielding them from foreign competition.[18] National security is sometimes mentioned as a driver, although as it is already well-recognized as a legitimate reason for making exceptions to cross-border date transfers in existing frameworks such as the APEC Privacy Framework, it will not be further discussed in this document.

Data localization may seem to provide a straightforward data policy solution for security or privacy related concerns. However, its effectiveness has been very limited and it is not consistent with the view of APEC on cross-border data flows, which the APEC Committee on Trade and Investment in launching the APEC Data Privacy Pathfinder has described as "the currency of the digital economy that fuels growth in the information age"[19]. APEC's view recognizes that organizations increasingly rely on data for many purposes and free and open trade and investment involving consumers cannot take place without the collection and sharing of personal data across borders. Preventing or placing burdensome restrictions on cross-border data flows most especially affects MSMEs that do not have the resources to deal with such restrictions in all jurisdictions where they have or wish to develop a customer base.

In addition, data localization carries with it significant costs and unintended consequences. A study

---

rt3.

[18] Joshua P. Meltzer and Peter Lovelock, ***Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia***. Brookings Institution Global Working Papers, March 18, 2018 [https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/]

[19] *APEC Data Privacy Pathfinder* (2007/CSOM/019). Paper submitted jointly by the Committee on Trade and Investment and the Electronic Commerce Steering Group to the Concluding Senior Officials' Meeting, Sydney, Australia, 2-3 September 2007.

by the European Centre for International Political Economy (ECIPE)[20] pointed to substantial negative impact of enacted or proposed data localization legislation on the economy in Brazil, China, the EU, India, Indonesia, South Korea and Vietnam (average of -0.7 percent of GDP). If applied across all sectors of the economy, GDP losses would be even higher (average of -1.04 percent). Nevertheless, concerns behind data localization are real and legitimate, and APEC needs to facilitate the development of sustainable and effective alternative solutions that can enable member economies to benefit from increasingly data-driven cross-border business activities. Such solutions could include a regional network that allows for the exchange of information, support effective cross-border enforcement and cooperation among jurisdictions.

In the banking sector, data localization creates tension between competing regulatory requirements and business inefficiencies on several fronts. For example, banks' obligations to comply with local personal data protection laws can conflict with international law enforcement requests. Banks ' threat responses are also hindered by restrictions on cross-border data transfers that limit the ability of a bank to share information on security threats between jurisdictions internally and externally. Cybersecurity can also be reduced due to the proliferation of data centers creating more attack vectors for nefarious actors to exploit. Many of the economic efficiencies that the Internet enables in the banking sector through the cross border nature of the service offering could also be eliminated. Lastly, regulations restricting cross border data transfers and regulations that require criminal reports to be made locally would limit banks' ability to report, for example, a criminal who has been rejected in one jurisdiction opening an account in another. The path forward should be one of enhanced collaboration among regulators in the region against cyber risks that minimizes data localization requirements.

To ensure that regulations are fit to purpose, it is important to clearly define objectives that jurisdictions are currently seeking to meet (e.g., protection of personal data, consumers and intellectual property, ensuring fair competition) and evaluate whether these objectives can be better met through data localization or through other measures.

- APEC economies should identify concerns that are currently being addressed or planned to be addressed through data localization, such as data privacy protection, maintaining cyber resilience, enabling access to data for law enforcement purposes, and the development of domestic technology and data-driven industries. They should evaluate whether these objectives can be better met through other measures that can go hand-in-hand with wider cross-border sharing of data, given the latter's critical importance to the realization of regional economic integration, the empowerment of MSMEs and sustained innovation and economic growth.

3.2. ADDRESSING CROSS-BORDER DATA PRIVACY PROTECTION

The extent to which personal information of individuals is protected is not increased by mandating data to be stored in a particular location. All domestic companies and most foreign companies are subject to the privacy laws and regulations of the jurisdiction where they operate and are bound to comply with these rules irrespective of where in the world the data are stored. Data localization cannot prevent a foreign company with no physical presence in the jurisdiction from collecting citizens' personal data when they visit its website; this can only be prevented by curtailing citizens' access to the Internet, which individuals and businesses will not consider practicable. The appropriate tools for ensuring cross-border data privacy are contracts and legal frameworks that set appropriate limits for voluntary disclosures of personal data.

To address cross-border privacy concerns, it is important for jurisdictions to agree on a common framework that enables cross-border data flow while assuring data protection. The EU's GDPR seeks to achieve this objective for the sharing of data within the EU, as well as for those that occur between organizations when one of them is based in the EU. Within the Asia-Pacific. the APEC Cross-Border

[20] Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde, ***The Cost of Data Localisation: Friendly Fire on Economic Recovery***. ECIPE Occasional Paper No. 3/2014.

Privacy Rules (CBPR) were introduced to provide a similar solution, without need for major changes in domestic law of member economies. However, the CBPR has to date made very limited progress – with only six member economies, around two dozen participating companies and two accountability agents currently in operation.

The CBPR faces challenges in attracting more economies and companies to participate. A few economies still do not have privacy laws. Most companies except the largest enterprises consider the cost of going through the certification process too high. Companies in emerging markets are also hesitant to shoulder the expense of participating in CBPR unless they see it attaining reciprocal recognition by the EU GDPR. Businesses consider the latter to be challenging due to their perception of a lower bar for CBPR compared to the GDPR and privacy frameworks in some advanced member economies.

Because many leading firms operating globally are based and regulated in the EU, which is also an important consumer market for Asia-Pacific companies, the GDPR is becoming a de facto global standard for cross-border privacy protection. Several APEC member economies have already completed or are undertaking gap analyses between their domestic privacy regimes and GDPR with the aim of becoming GDPR-compliant. These efforts will help facilitate cross-border data flows between these economies and the EU. However, APEC needs to accelerate the development of its own regional privacy framework to facilitate such flows among its member economies in order to achieve economic integration. This is particularly important for developing economies and their smaller banks, fintech start-ups and MSMEs that are internationally active, which will be impacted most by the introduction of GDPR, as they do not have sufficient resources to devote to stringent compliance procedures.

Ways forward to develop such a framework need to be considered. One is to undertake gap analyses between CBPR (and the underlying APEC Privacy Framework) and the privacy regimes of participating economies, and between CBPR and GDPR, in order to identify areas where derogations (flexibility to add or modify certain provisions of the regional regime to fit local needs and laws) can be applied or where specific measures are needed to achieve inter-operability and thus attract more companies to participate. To enable MSMEs to participate, the feasibility of a lighter, lower-cost version of CBPR should be explored. CBPR could also be given more visibility by creating a globally recognizable special designation for companies that have achieved compliance (which currently is done by listing them in the CBPR Compliance Directory).

Moving towards a regional privacy regime that is inter-operable with GDPR is a step that needs to be taken. The APEC Privacy Framework and CBPR are foundations on which this regime can be built, but this effort can only succeed if a critical mass of companies and jurisdictions come to have sufficient confidence in and participate in CBPR. More thinking is also needed to help expand access to data that may be useful to businesses and that can be shared across borders. For example, data classification solutions and technologies that anonymize or encrypt data could facilitate these goals. Rules and regulations need to be reformed to allow the use of technologies and solutions in enabling wider cross-border sharing of data, including personal data.

While harmonization as an approach to a regional regime is very difficult if not impossible to attain, greater coordination is achievable and should be the focus of efforts, in particular with respect to the different legal approaches in this very diverse region. The GDPR, being a set of principles, norms and values, is becoming a driver of this process, as a number of jurisdictions in APEC see themselves compelled to work with the EU towards compliance with the GDPR's adequacy requirements. A practical way forward for APEC economies in developing a regional data regime that facilitates data sharing across their markets is to promote improved compatibility of laws and values.

It will take time for a regional privacy regime to develop. In the meantime, jurisdictions in the region can explore other approaches that can facilitate cross-border data flows among those interested. One possible approach would involve bilateral or plurilateral memoranda of understanding. Another approach, which could also be combined with the bilateral or plurilateral MOU, is agreement on a

negative list. A pilot project aiming to promote the cross-border sharing of credit scores among credit bureaus in the Mekong subregion is being undertaken by APFF, which could eventually be expanded in scope.

Proposed actions:

- APEC should complete a gap analysis between the CBPR/APEC Privacy Framework and the GDPR and identify steps to achieve inter-operability between the two frameworks. Parallel to this effort, APEC should provide a platform for member economies who agree to undertake thorough gap analyses between their domestic privacy regimes and the CBPR/APEC Privacy Framework. The gap analyses should aim to identify the areas where domestic regimes are comparable to the CBPR/APEC Privacy Framework as well as the areas where gaps exist, and develop measures to address those gaps to enable recognition that CBPR-certified organizations meet domestic legal standards. These gap analyses should involve collaboration among relevant government agencies and regulators, the private sector and international organizations, including the APFF.

- APEC should promote broader industry participation in the CBPR by introducing mechanisms that would allow MSMEs to participate (e.g., a lower-cost version of the CBPR) and creating a globally recognizable certification mark to attract more companies to apply for certification as CBPR-compliant.

3.3. Addressing Data Security Protection

Promoting data security requires establishing a comprehensive set of controls to prevent the inadvertent disclosure of data such as, for example, through hackers penetrating an organization's network or employees mistakenly or deliberately posting sensitive information on social media. Location has no impact on security – data localization cannot prevent security breaches if an organization in the jurisdiction fails to maintain such controls, as such breaches can occur anywhere in the world, regardless of where data are stored.

Data localization could also have unintended negative consequences for data security.

- For example, cloud computing is becoming important for MSMEs that rely on large-scale cloud-computing services in other jurisdictions to offer them strong data security programs that they cannot afford to implement in-house. Requiring firms to use data centers located within the jurisdiction will increase costs, while denying these firms the opportunity to access the most secure and affordable cloud computing services wherever they are available irrespective of the location.

- A second example is access to new technological innovations, including data security. Barriers to cross-border data flows prevent domestic organizations from accessing data, which are important for research and development and the creation of new innovative products and services. Where such barriers prevent access of domestic players to new and updated technologies and facilities and cross-border innovation, they result in eventually weakening protection against increasingly sophisticated fraud and threats to privacy and security of citizens' data.

- A third example is disaster resilience. By preventing data from being backed up in other parts of the world, localization could weaken resilience of organizations against natural catastrophes such as earthquakes that may result in destruction of data within a jurisdiction.

Economic growth powered by digitization has resulted in transformation of the supply-chain landscape in various industries. APEC economies should consider the maturity of security programs across the board before adopting localization requirements. As has been demonstrated in various breaches reported in recent years, a weakness found in a vendor network could potentially be exploited to cause harm to organizations in an unrelated industry. Empowering organizations to

choose vendors that respect and implement strong security controls irrespective of their location should be encouraged.

Organizations face growing threats to data security, as the number of data breaches and records lost and cases of cybercrime continue to rapidly grow over recent years. The need for public-private collaboration in building a stronger foundation for data security is becoming more acute as vulnerabilities increase with the growing adoption of cloud, big data, Internet of Things and mobile payments by enterprises. In particular, there is a great need in the region for:

- A long-term strategy for managing the data security environment, including standardization of data protection laws, partnership among institutions and sharing of experiences;
- Comprehensive guidelines on data security and business continuity among others, utilizing technological advancement as well as regulatory collaboration and peer learning;
- Wider intelligence-sharing among jurisdictions, which requires higher levels of trust among them that would also be important to facilitate emergency responses;
- Innovative programs for security in payments and other industries that are the being increasingly targeted by cyber criminals;
- Development of expertise in cybersecurity to transform and upgrade current systems;
- Regulatory sandboxes where innovations can be tested before being fully brought to the market;
- Greater recognition by companies' boards of directors of cyber resilience and privacy as priority issues; and
- Capacity building that involves existing resources and expertise in the private and public sector as well as in international organizations).

Keeping personal data secure is a risk-based process, involving reasonable procedures based on best practices in an appropriate and "evergreen" standard. These include public key cryptography,[21] public key infrastructure (PKI),[22] encryption of data at rest and in transit,[23] and emerging innovations in data security. Member economies can benefit from capacity building measures to assist them in enhancing data security. This may involve the adoption of cutting-edge cloud solutions to avoid creating a single point of attack and strengthening data security in business process outsourcing organizations.

Data Governance (or management) is central to resolving existing concerns around the free flow of data across borders, as well as in the sharing, storage and use of data in-country. Specifically, many governments are concerned about the potential for increased cyber risk resulting from the offshore transfer, processing and storage of data, which has also given way to concerns around the privacy of an economy's citizens. Data classification frameworks can be a useful tool to establish domestic and cross border data regimes to govern the acceptable use and protection of data. Furthermore, by dividing data into distinct categories based on sensitivity levels and risk profiles, appropriate security controls can be determined, leading to a risk-based approach to cybersecurity while also helping to allay privacy concerns.

Ensuring that both fintech firms and traditional firms abide by the same classification frameworks will also be important. A regional approach to data classification would further help to overcome the potential problem of incompatible classification frameworks which could present additional problems in future. Data classification frameworks will also assist in public cloud adoption by governments which can help to power e-government services, including those relevant to financial services.

---

[21] Public-key cryptograhy (also known as asymmetric cryptography), is a system that uses a pair of keys: a public key that is widely disseminated, and a private key known only to the owner. This enables both authentication (by verifying that a holder of the paired private key sent the message) and encryption (as only the private key holder can decrypt the encrypted message).

[22] Public key infrastructure (PKI) is a system for creating, managing, distributing, using, storing and invalidating digital certificates and managing public-key encryption.

[23] Data at rest refer to data that are physically stored in any digital form, while data in transit are data that are flowing over networks, which may be public (e.g., the Internet) or private (e.g., a corporate or enterprise local area network).

Proposed action:

- APEC should develop a long-term strategy for strengthening data security in the region by convening a series of conferences and discussions among relevant experts from the public and private sectors, global standard setters such as the ICCR and international and academic institutions toward this end. This strategy could include, among others, the adoption of baseline agreed standards on cybersecurity, the development of comprehensive guidelines on data security and business continuity that balances innovation and safety, expansion of intelligence-sharing on cybercrime, development of innovative programs for promoting security in the payments and lending industries especially in encryption and authentication, the use of regulatory sandboxes to develop innovative digital products and services while ensuring that appropriate protections and safeguards are in place, the design of incentives for company directors to treat cyber resilience and privacy as priority issues, and leveraging existing resources and international expertise for capacity building of regulators.
- Individual jurisdictions should review cyber resilience legislation involving all major relevant stakeholders in the public and private sectors and introduce reforms where needed. The industry should complement the legislation with a set of industry best practices developed at the regional level.

3.4. Facilitating access to data for law enforcement purposes

Data localization requirements for law enforcement purposes aim to enable local authorities to directly compel domestic companies or subsidiaries of foreign firms to provide data to law enforcement authorities. This trend has been a response to the ineffectiveness of the Mutual Legal Assistance Treaty (MLAT) system – for many years the system of international agreements among jurisdictions to assist each other in law enforcement – which has already been overwhelmed by the explosion and rapid expansion across the entire world of digital information used for criminal investigation and prosecution, as well as new uncertainties surrounding the impact of new privacy and data protection regulations across jurisdictions on the MLA process.

The use of data localization requirements for law enforcement purposes as an alternative to the slow MLA process creates potential problems as companies become subject to multiple and competing jurisdictions and could force firms to leave markets. A better alternative would be to increase funding for the MLA process and/or reform and streamline the MLA to unclog the system and shorten the time to access data, e.g., expedited access to jurisdictions meeting agreed international standards, streamlining multiple and redundant request reviews, narrowing down the types of allowable requests for stored data, introduction of online forms and promoting their use at the global level.

International data sharing could also be enhanced through international agreements that can provide mechanisms for law enforcement authorities to access data held in another jurisdiction. The recently passed Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in the USA provides an example of a mechanism that authorizes the US Department of Justice to enter into executive agreements with foreign government agencies and enable foreign jurisdictions to enforce their laws vis-à-vis US service providers.

Public and private sector partnerships have been another way to facilitate greater information sharing between law enforcement entities, government departments and private companies. In 2017, three new Financial Information Sharing Partnerships (FISPs) were launched in Asia-Pacific: the Fintel Alliance in Australia, the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) in Singapore; and the Fraud and Money Laundering Intelligence Taskforce (FMLIT) in Hong Kong. These had direct positive results and demonstrated how organizations could meet law enforcement goals without sacrificing data privacy or security. Laws that develop barriers to information sharing threaten the development of these tools to fight financial crime more effectively.

Proposed action:

- Governments should reform the Mutual Legal Assistance Treaty (MLAT) system to streamline the process of providing cross-border access to law enforcement officials to digital information for criminal investigation and prosecution purposes. Various reform proposals that have been put forward should be considered, particularly the use of online forms. As the process of reforming the MLAT system may take several years, member economies should also consider undertaking and expanding international agreements for law enforcement authorities to have access to relevant data in each other's jurisdictions. Governments should develop partnerships where possible within existing laws to allow for greater coordination and cooperation between the public and private sector.

3.5. Promoting the development of the Domestic Data infrastructure and data-driven and technology industries

Among the considerations behind data localization is the role it could play in stimulating the development of domestic infrastructure and data-driven industries and employment, as foreign firms are compelled to establish a presence inside the jurisdiction and domestic companies are set up to meet the captive local demand for data storage and processing. While similar approaches used in non-digital contexts, such as behind-the-border regulations and local content and technical requirements have had some success in a few economies, it is not clear whether this can produce similar results for digital products and services.

For example, the increasing automation of data centers has reduced their potential for creating jobs in communities where they are established. As mentioned in a previous section, barriers can prevent domestic organizations from accessing data, which are important for research and development and the creation of new innovative products and services. Together with higher costs of services compared to competitors in other jurisdictions, these could make it more difficult to develop a domestic industry that can compete internationally on its own.

Where data localization has the effect of protecting domestic companies from online competition, the risk arises of the policy being judged as inconsistent with the jurisdiction's commitments under the WTO and opens the economy to potential retaliation by trading partners. Data localization could limit economies' ability to generate value from cross-border data flows. These are especially relevant to MSMEs that would benefit from ready access to global service delivery platforms, as well as to digitally intensive firms that contribute significantly to economic growth, wages and employment.[24]

Data localization has also been seen as a way to limit the activities of new foreign digital entrants that use domestic communications infrastructure but do not pay license fees and are not subject to regulations of content and operations. However, it could have the unintended consequence of also limiting the potential for infrastructure investment and upgrading. The experience so far has shown that after new digital entrants invest in infrastructure to improve services, consumers become more willing to pay to upgrade internet connections, thus creating a virtuous cycle.

A part of the economy that is growing in importance in emerging markets is the new Digital Supply Chain, where the flow of physical goods is enabled by the information flow that results in increased trade. Within this supply chain, businesses are increasingly using online marketplaces and payment systems to transact, advertise and grow their business. This process is being enabled by e-commerce and e-payment platforms that are providing low-cost marketing services, which enable many MSMEs to join cloud-based private or public global value chains. In most emerging markets, however, much remains to be done to build digital infrastructure.

[24] Examples of this impact are the following: (a) Local companies may be required to pay 30 to 60 percent more for their computing needs than if they were able to choose more freely. (b) Data breaches may become more costly given the limited recovery options, which would particularly impact smaller economies. (c) Limits to cross-border data flows act as non-tariff barriers that increase the level of geographic isolation from export markets, particularly of smaller economies.

Local data storage requirements and restrictions on cross-border data flows impact digital trade by increasing costs, reducing service suppliers' ability to realize economies of scale, and discouraging investment. Examples are requirements for Internet service providers to store retained subscriber traffic data within the jurisdiction, for business records to be stored in the jurisdiction even when low-cost cloud services are used, and for personal financial information collected in the jurisdiction to be stored locally.

Proposed action:

- Member economies should develop domestic data-driven industries by developing a holistic set of enabling policies and measures, including educational measures and the expansion of digital infrastructure, to help entrepreneurs and workers benefit from digital trade opportunities, and ensuring that they have access to the data and technologies they need, based on the APEC Blueprint for Action on Electronic Commerce,[25] and the APEC Best Practices to Create Jobs and Increase Competitiveness.[26]

3.6. Establishing Regional Platforms for Enabling Appropriate Use of New Technologies in Cross-Border Financial Services

The deployment of new platforms, processes and systems such as blockchain, APIs/open banking, cloud computing, data analytics and artificial intelligence raise concerns among regulators regarding its implications on cross-border data flows. The cross-border data flow nature of these operating models can cause a blurring of jurisdictional borders, raising questions regarding which set of laws and regulations are applicable and which authorities are responsible for ensuring market integrity, protection and safeguards. There is a risk that the opacity of these technologies, ranging from cryptography to statistical models and codes, can create a blind reliance by users on these technologies, giving rise to a lack of clear accountability, recourse and enforcement processes in the event of willful manipulation. There are also currently no clear cross-jurisdictional rules to address the misuse of cross-border data.

These challenges are further exacerbated by the fact that technologies develop faster than traditional legislative and other rule-making processes, giving rise to the problem of policy responses are no longer relevant or effective by the time they are put in place. Another related challenge is the

[25] The Blueprint defines the role of governments as promoting and facilitating the development and uptake of electronic commerce by : (a) providing a favourable environment, including the legal and regulatory aspects, which is predictable, transparent and consistent; (b) providing an environment which promotes trust and confidence among electronic commerce participants; (c) promoting the efficient functioning of electronic commerce internationally by aiming, wherever possible, to develop domestic frameworks which are compatible with evolving international norms and practices; and (d) becoming a leading-edge user in order to catalyze and encourage greater use of electronic means. It calls on business and government to cooperate wherever possible to ensure the development of affordable, accessible and interoperable communication and information infrastructure and to co-operate to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy, authentication and consumer protection. While recognizing that some degree of government regulation may be necessary, the Blueprint advises economies to favor technology-neutral, competitive market-based solutions which can be safeguarded by competition policy, and effective industry self-regulation.
[https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx]

[26] Annex F of the 2013 Joint Statement of the APEC Ministers identified the following best practices: (a) making economies cost-competitive for production by promoting an internationally attractive business environment and supporting investment in infrastructure development; (b) spurring innovation through new technologies by promoting research collaboration and providing effective protection and enforcement of IPRs; (c) attracting investment by improving the investment climate, investing in education and workforce training, strengthening manufacturing supply chains and improving logistics and promoting access to the digital economy; (d) addressing market access barriers; and (e) assisting SMEs by increasing SMEs' export opportunities, facilitating SMEs' access to supply chains, facilitating SMEs access to capital and to emerging technologies, and providing SME manufacturers information and tools to improve efficiency and profitability
[https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2013/2013_amm/annexf].

scarcity of human resources with specialized technical expertise to deal with the impact of current and future emerging technologies on financial services.

Collaboration among regulators and industry to deal with these challenges will require the establishment of a regional platform that aims to facilitate innovation in cross-border financial services as well as cross-border cooperation. This platform should include financial services providers, including incumbent banks, fintech companies and information service providers. Platforms that also provide opportunities for regulators to observe actual business operations using the latest available technologies could significantly improve their capacity to provide an enabling environment for innovation in financial services.

The ASEAN Financial Innovation Network (AFIN) provides an example of such a platform. AFIN is a collaborative platform that brings together banks, microfinance institutions, non-banking financial institutions and fintech firms from the region to facilitate the adoption of innovations by financial service providers, accelerate business and product development, the adoption and convergence of APIs and promote development of IT architecture strategy and management skills in financial institutions. AFIN includes a sandbox that allows regulators to observe the activities of industry participants and their impact on key issues such as security, data privacy and consumer protection and provides opportunities for policy harmonization and partnerships among them.

It is also important to introduce domestic sandboxes which both incumbents and new entrants can utilize so that innovative fintech solutions that might not otherwise fit into existing regulations can be explored and progressed with regulators. In some jurisdictions this might mean separate sandboxes for banking, securities and insurance. In other jurisdictions these could be combined. There are already a number of positive examples of domestic sandboxes in APEC economies, including in Singapore, Hong Kong, Indonesia, Korea, Malaysia, Thailand. Vietnam and China are considering launching as well.

Establishing linkages between domestic sandboxes in APEC and beyond is also important. Firms can benefit from streamlined approval processes and government can benefit from the experience of others. With such linkages successful innovations in one economy can be utilized by others without long waiting periods or a jurisdiction by jurisdiction approach having to be adopted. A network of MOUs are currently being built across the region including bilateral agreements among Australia, Hong Kong, Malaysia, Singapore, Thailand, Brunei, Philippines, Vietnam as well as outside of the region with Dubai, France and the UK which can be built on.

Proposed actions:

- APEC economies should develop regional public-private sector platforms to enable policies and regulations that can facilitate cross-border flows of financial services and data through the promotion of existing and development of new minimum benchmarks. Key objectives that could be pursued through these platforms are: (a) a framework of shared accountability and responsibility that can guide financial service industry players that are rapidly adopting tech-based models; (b) pool scarce human resources who can support policy and regulatory awareness and development, such as in translating principles-based regulations into implementable and practical requirements; (c) the design of principles-based legislation and regulations; (d) establishment of a clear consumer recourse process to support the uses of data analytics and intelligence; and (d) coordination among regulators and industry in the region in developing industry codes and standards to complement and support legal and regulatory frameworks.

- Introduce regulatory sandboxes that both incumbents and new entrants can utilize and that are coordinated across jurisdictions wherever there is potential to facilitate the development of innovative financial services. APEC should also support and build on existing MOUs; to look at where the gaps and roadblocks would be for fintech firms in either market to gain approvals and be able to enter the other after having met necessary requirements during sandbox experimentation; and to look to broaden the MOUs out to include multiple economies.

APPENDIX A

CONFERENCE SPEAKERS AND MODERATORS AND CONFERENCE CALL PARTICIPANTS

Conference Calls:

1. May 8, 2018 – Role of Data, Current Landscape for the Data Industry, Technology and Regulations
2. May 17, 2018 – Domestic Data Regulation
3. May 25, 2018 – Cross-Border Data Access
4. May 31, 2018 – Uses of Data
5. June 13, 2018 – Level Playing Field

Conference: Charting a Roadmap Toward a New Data Regime for the Digital Economy
June 20-21, 2018, Mochtar Riady Auditorium, Singapore Management University

Name	Organization	Position	Conference Calls					Conference Speaker
			1	2	3	4	5	
Allan Bollard	APEC Secretariat	Executive Director						■
Lawrence Low	Allen & Gledhill Regulatory & Compliance Pte Ltd	CEO						■
Raymond Li	Ant Financial Services Group	General Manager, Legal and Compliance Department						■
May-Ann Lim	Asia Cloud Computing Association	Executive Director						■
Michael Mudd	Asia Policy Partners LLC	Managing Partner			■			
Peter Tierney	AxiomSL	CEO, APAC						■
Tod Burwell	BAFT	President and CEO		■	■	■		
John Ott	Bain & Co.	Partner	■				■	■
Peter Sheerin	Business Information Industry Association (BIIA)	Committee Chair, Asia-Pacific Consumer Credit Information	■	■				■
Ken Katayama	Center for Financial Industry Information Systems, Japan	Director of International Industry Information Systems	■	■	■	■	■	
Peter Douglas	Chartered Alternative Investment Analyst Foundation	Director						■
Catherine Simmons	Citi	Managing Director and Head of Government Affairs	■	■		■		■
James Bond	Citi	Head of Government Affairs, Australia				■		
Kimberley Claman	Citi	Director, International Government Affairs				■		■
Chee Kin Lam	DBS Bank Ltd	Managing Director & Head, Group Legal, Compliance & Secretariat						■
Piyush Gupta	DBS Group	CEO and Director						■
Jean-Remi Lopez	DTCC	Director of Government Relations - Asia						■
Oliver Williams	DTCC Data Repository Services Singapore	CEO						■
Catherine Khaw	Data & Analytics Capital	Founder and Chief Intelligence Officer						■
Peter Leonard	Data Synergies	Principal			■		■	■
Boon-Hiong Chan	Deutsche Bank	Director and Head – Market Advocacy APAC/MENA	■					■
Wijaya Abori	Deutsche Bank	Regional Data Privacy Officer, APAC and Senior Counsel						■
Charmian Aw	Drew & Napier LLC	Director, Telecommunications, Media and Technology						■
Poh Lip Hang	Drew & Napier LLC	Assistant Head, Competition & Regulatory Economics						■
Tju Liang Chua	Ethereum Foundation	General Counsel						■
Francis Gross	European Central Bank (ECB)	Senior Adviser, Directorate General Statistics						■
Anthony Hadley	Experian	Vice President, International Policy				■		■

George Shand	FICO Scores	Senior Director, Americas				■		
Umang Moondra	Fidor	APAC Head						■
Toshiki Yano	Google	Head of Privacy and Security, APAC	■	■	■			■
Eugenio Briales Gomez Tarragona	Harvard Law School	Visiting Professor	■		■			
William Hallatt	Herbert Smith Freehills	Partner						■
Luz Maria Salamina	IFC/World Bank Group	Lead Financial Sector Specialist		■		■		
Jinchang Lai	IFC/World Bank Group	Principal Operations Officer		■	■		■	■
Hung Ngovandan	IFC/World Bank Group	Principal Financial Specialist		■				■
Rishi Kapoor	ISDA	Director, Policy, Asia-Pacific						■
Zhijian Liu	JD Finance	General Counsel						■
Gerard George	Lee Kong Chian School of Business, SMU	Dean/Professor of Innovation and Entrepreneurship						■
Yi Lin Seng	Mastercard	Senior Managing Counsel						■
Julius Caesar Parreñas	Mizuho	Senior Advisor	■	■	■	■	■	■
David Hardoon	Monetary Authority of Singapore	Chief Data Officer						■
Brian Yeoh	Monetary Authority of Singapore	Deputy Director, Data Governance & Architecture						■
Surapol Opassatien	National Credit Bureau Co Ltd	CEO						■
Donald MacDonald	OCBC Bank	Head, Group Customer Analytics & Decisioning						■
Phoram Mehta	PayPal	Head of Information Security			■	■	■	■
Yeong Zee Kin	Personal Data Protection Commission	Deputy Commissioner						■
Gloria Pasadilla	Policy Support Unit, APEC	Senior Analyst	■			■		■
Michael Turner	Policy and Economic Research Council (PERC)	President	■			■	■	
Patrick Walker	Policy and Economic Research Council (PERC)	Director of Research				■	■	■
Luther Moncrief	SAP Asia	Solution Adviser Expert, Database & Data Mgt.						■
Matthew Gamser	SME Finance Forum / IFC	CEO			■			■
Lisa O'Connor	SWIFT	Head of Standards, APAC	■	■				
Ekkehart Boehmer	Sim Kee Boon Institute for Financial Economics, SMU	Academic Director						■
Shameek Kundu	Standard Chartered Bank	Chief Data Officer						■
Alexander Helter	Stradegi Consulting	Senior Business Consultant						■
Jianshu Weng	Swiss Re Asia Pte Ltd	Senior Analytics Specialist						■
Peter Lovelock	TRPC Pte. Ltd.	Director and Founder	■		■			
Laura Winwood	TRPC Pte. Ltd.	Director	■	■		■		
Douglas Arner	The University of Hong Kong	Kerry Holdings Professor in Law						■
Daniel Warelis	Thomson Reuters	Government and Regulatory Affairs	■		■	■		■
Julia Walker	Thomson Reuters	Head of Market Development, Risk & Regtech, Asia		■				
Celina Leung	TransUnion	Vice President and General Counsel, Asia-Pacific		■				
Richard Lowe	UOB	Group Chief Data Officer						■
Matthew Mohlenkamp	US Department of the Treasury	Financial Attache for Southeast Asia	■	■			■	
Carol Cohen	US Department of the Treasury	International Economist	■					
Kay Turner	US Department of the Treasury	Economist	■	■	■	■	■	
Amy Zuckerman	US Department of the Treasury	Presidential Management Fellow		■	■			

ADVISORY GROUP
MEETING PAPER 3-B

An APEC Roadmap for a New Financial Services Data Ecosystem

APPENDIX B

CONFERENCE PROGRAM

Charting a Roadmap Toward a New Data Regime for the Digital Economy

(8th Annual SKBI Conference 2018)
June 20-21, 2018, Mochtar Riady Auditorium, Singapore Management University

Organizers:
APEC Business Advisory Council (ABAC) / Asia-Pacific Financial Forum (APFF)
Sim Kee Boon Institute for Financial Economics, Singapore Management University (Host)
International Finance Corporation (IFC) / World Bank Group
Supported by:
Monetary Authority of Singapore (MAS)
Deutsche Bank

20 June 2018, Wednesday

Time	Session	Speakers
09:00 – 09:05	Introductory Remarks	Ekkehart Boehmer Academic Director, Sim Kee Boon Institute for Financial Economics Keppel Professor of Finance, Singapore Management University
09:05 – 09:10	Welcome Address	Gerard George Dean and Lee Kong Chian Chair Professor of Innovation and Entrepreneurship, Lee Kong Chian School of Business, Singapore Management University
09:10 – 10:25	Session 1 The Evolving Data Landscape Panel A: The Evolving Data Industry and Technology Landscape What are the new and emerging technologies, and how are they affecting data? With greater uses of non-traditional sources of data, and the rise of the data analytics industry, should there be a separate "Data industry"? Should Data should be treated as a public good. If so, what kind of Data and what are the acceptable trade-offs between data as a public good and data privacy? What is Data's spill-over effects on the financial industry and other industries? What to measure? Which industries / firms / departments are likely to find it easier to adapt to data-driven economics? Q&A	Moderator Patrick D Walker, Director of Research, PERC Panelists David Hardoon, Chief Data Officer, Data Analytics Group, Monetary Authority of Singapore Zhijian Liu, General Counsel, JD Finance John Henry Ott, Director, Bain & Co. Inc Jianshu Weng, Senior Analytics Specialist, Digital and Smart Analytics, Swiss Re Asia Pte. Ltd
10:25 – 10:45	Tea Break	
10:45 – 12:00	Session 1 The Evolving Data Landscape Panel B: The Evolving Regulatory Landscape around Data. How does the existing regulatory landscape around Data look like? What are the challenges and trends? What are the inhibitors to unlocking the greater potential of data for financial services in the context of current laws, regulations, institutional structures and industry practices, strategic concerns and government interventions e.g., Privacy, AnaCredit, PCR, Open	Moderator Julius Caesar Parrenas, Coordinator, Asia-Pacific Financial Forum and Senior Advisor, Mizuho Bank, Ltd Panelists Douglas Arner, Kerry Holdings Professor in Law, The University of Hong Kong

Time	Session	Speakers
	Data Initiative, APEC-CBPR, country's laws and regulations. Q&A.	Raymond Li, General Manager, Legal and Compliance Department, Ant Financial Services Group Richard Lowe, Group Chief Data Officer, UOB Patrick D Walker, Director of Research, PERC
12:00 – 13:00	Networking Lunch	
13:00 – 14:15	Session 2 Domestic Data Regulation Panel A: How to develop a coordinated, holistic and dynamic data regulatory approach? What can be coordinated regulatory approaches to the Data lifecycle including data resilience? There is an emergence of many new market players offering data analytics services. What the regulatory challenges and approaches? Can domestic policies and regulations concerning financial services data be modularised and harmonised to better support a coordinated, holistic and dynamic approach? How? Q&A	Moderator Boon-Hiong Chan, Director, Head of Market Advocacy, Business Control Unit, Global Transaction Banking, Deutsche Bank AG Singapore Panelists Francis Gross, Senior Adviser, Directorate General Statistics, European Central Bank Alexander Helter, Senior Business Consultant, Stradegi Consulting Jinchang Lai, Lead Financial Sector Specialist, and Lead for Financial Infrastructure, East Asia & Pacific, International Finance Corporation (IFC), World Bank Group Peter Leonard, Principal, Data Synergies Pty Limited
14:15 – 15:30	Session 2 Domestic Data Regulation Panel B: How domestic regulation can respond to globalisation of business? What is the applicability of physical data sovereignty in a virtual borderless world? To what extend should a regulator have extra-territoriality reach outside of its physical border over data. What are the implications of EU GDPR, USA CLOUD ACT, APEC CBPR and other Asia country's regulations on Asia Pacific financial services industry? Q&A.	Moderator Gloria O. Pasadilla, Senior Analyst, APEC Policy Support Unit Panelists Hùng Ngovandan, Lead Financial Sector Specialist, International Finance Corporation, World Bank Group Peter Sheerin, Executive Committee Member, Business Information Industry Association Catherine Simmons, Head of Government Affairs for Asia Pacific, Citibank
15:30 – 15:50	Tea Break	
15:50 – 17:05	Session 2 Domestic Data Regulation Panel C: How domestic regulation can respond to increasing data volume and complexity? What are the potential key economic consequences of increasing data volume and complexity? The revisions and addition of regulations require resources, new ways of thinking and the potential of new frauds require new enforcement processes. To what extent does increasing data	Moderator Dan Warelis, Government and Regulatory Affairs, Asia-Pacific, Thomson Reuters Panelists Rishi Kapoor, Director, Policy, Asia Pacific, International Swaps and Derivatives Association, Inc. (ISDA)

Time	Session	Speakers
	volume and complexity affect the net cost of compliance and risks for the involved parties? Q&A.	Chee Kin Lam, Managing Director & Head, Group Legal, Compliance & Secretariat, DBS Bank Ltd Surapol Opassatain, Chief Executive Officer, National Credit Bureau Co., Ltd
17:05 – 17:10	Closing Remarks for Day 1	Ekkehart Boehmer Academic Director, Sim Kee Boon Institute for Financial Economics Keppel Professor of Finance, Singapore Management University
19:00 - 21:00	Dinner (for invited guests only)	Welcome Remarks by Alan Bollard Executive Director, the APEC Secretariat, Singapore

21 June 2018, Thursday

Time	Session	Speakers
08:30 – 08:35	Welcome Address	Piyush Gupta Chief Executive Officer and Director, DBS Group Chairman of Advisory Board, Sim Kee Boon Institute for Financial Economics, Singapore Management University
08:35 – 09:35	Keynote Speech: Trust and Progressive Data Protection for Innovation	Yeong Zee Kin Assistant Chief Executive (Data Innovation and Protection Group), Infocomm Media Development Authority of Singapore Deputy Commissioner, Personal Data Protection Commission
09:35 – 10:45	Session 3 Cross Border Data Access Panel A: How to address concerns driving localisation? What are the causes for localisation effects on data? How does laws and regulations create localisation effects and when does localisation prevents cross-border data flows? What can be done to address these concerns and to streamline the current laws and regulations giving such effects? Q&A.	Moderator Jean-Remi Lopez, Director of Government Relations - Asia Pacific, DTCC Panelists Phoram Mehta, Head of Information Security, APAC, Paypal Pte Ltd Toshiki Yano, Public Policy and Government Relations Counsel, Strategy and Operations, Google APAC Yi Lin Seng, Senior Managing Counsel, Mastercard
10:45 – 10:55	Tea Break	
10:55 – 12:05	Session 3 Cross Border Data Access Panel B: How to develop policy and/or regulatory approaches for Cloud, Blockchain, Data Analytics/Intelligence and Fintech/Open Banking services? This panel combines technology, business model and legal/regulatory views.	Moderator Boon-Hiong Chan, Director, Head of Market Advocacy, Business Control Unit, Global Transaction Banking, Deutsche Bank AG Singapore

	How are technologies being deployed, the new and emerging operating models? What are the policy and regulatory considerations of case studies including: Cloud – how to approach data residency, data at rest, in transit and access to data stored in multiple locations. (Public) Blockchain & "Cryptos" - how to approach privacy & confidentiality when regulations require transparency, fit with key regulations with its cross-border decentralised processing, virtual participations and non-human readable scripts. Data Analytics and Intelligence - how to approach data analytics and intelligence, what are the current advances, risks and vulnerabilities; emerging markets' considerations, when financial services models are used in cross-border/different jurisdictions and how can unintended effects be practically detected? Opening Banking Application and Cross-border Application Programme Interface (API) uses; How to realise scalability for fintech service providers who are in one country and its users are in another country. The benefits of API and Open Banking, what can be a balance of responsibilities in the uses of data used for banking services - by banks, service providers and Application Programming Interface (API) fintech users. Q&A	Panelists Tju Liang Chua, General Counsel, Ethereum Foundation William Hallatt, Partner, Herbert Smith Freehills Catherine Khaw, Founder and Chief Intelligence Officer, Data & Analytics Capital Lim May-Ann, Executive Director, Asia Cloud Computing Association, and Managing Director, TRPC Pte Ltd
12:05 – 13:00	Networking Lunch	
13:00 – 14:00	Session 3 Cross Border Data Access Panel C: How to develop regulatory and standardised approaches to cross-border data flows, data classification and storage? This panel will combine technology and legal/regulatory views. How should the concept of "Jurisdiction" be defined since data flows and/or storage can cover several countries at the same time. What are the key definitions and classifications (e.g. "anonymised data", "confidential" data, "national interest data") that need consistent interpretation across borders; why? What roles can advance technology play? What and how frameworks and standards be developed to support financial data's cross-border flows? Q&A.	Moderator Charmian Aw, Director, Telecommunications, Media and Technology, Drew & Napier LLC Panelists Kimberley Claman, Director, Global Government Affairs, Citigroup Inc. Luther L. Moncrief, Solution Adviser Expert, Database & Data Management COE, SAP Asia Oliver Williams, CEO, DTCC Data Repository Services, Singapore
14:00 – 15:00	Session 4 Uses of Data Panel A: How to ensure confidence and trust in algorithms? Confidence and trust in algorithms will underpin the further development of the financial services sector, and as such, the ethical uses of data will be important. What are the elements of ethics for using algorithms to deliver financial services? How can key elements like Transparency, Accountability and Remediation processes be defined? To what extent should we rely on industry standards, codes of ethics and practice versus regulatory requirements on the uses of data? Q&A.	Moderator Brian Yeoh, Deputy Director, Data Governance & Architecture Office, Data Analytics Group, Monetary Authority of Singapore Panelists Shameek Kundu, Chief Data Officer, Standard Chartered Bank Lawrence Low, Chief Executive Officer, Allen & Gledhill Regulatory & Compliance Pte. Ltd. (AGRC)
15:00 – 15:15	Tea Break	
15:15 – 16:30	Session 4 Uses of Data Panel B: How to balance consent and data granularity in	Moderator Peter Douglas, Director, CAIA (Chartered Alternative Investment Analyst) Foundation

	practical ways? What is personal data? Should public cryptographic attributes be a part of personal data? For personal data, derived data and consent, what should be a balance between consent and level of granularity before Consent becomes overly onerous for all? How is this being done now? What would be considered as excessive levels of data collection and appropriate levels of data granularity for financial services? Any technology solutions? Q&A.	Panelist Wijaya Abori, Regional Data Privacy Officer APAC and Senior Counsel, Deutsche Bank Tony Hadley, Senior Vice President, Government Affairs and Public Policy, Experian Donald MacDonald, Head, Group Customer Analytics & Decisioning, OCBC Bank
16:30 – 17:30	Session 4 Uses of Data Panel C: What are the standards on owners, users and 3rd parties to use and share data and derived data? Who owns derived data generated from other data? How should data owners, processors and 3rd parties share data? Should data subjects be paid? What are the data-related legal and regulatory considerations when different industries uses similar data sets for financial services purposes? What are the challenges to "fair competition" in the age of Data? Q&A.	Moderator Matthew Gamser, CEO, SME Forum, International Finance Corporation (IFC), World Bank Group Panelist Umang Moondra, APAC Head, Fidor Poh Lip Hang, Assistant Head, Competition and Regulatory Economics, Drew & Napier LLC Peter Tierney, CEO, APAC, AxiomSL
17:30-17:45	Closing Remarks	Ekkehart Boehmer Academic Director, Sim Kee Boon Institute for Financial Economics Keppel Professor of Finance, Singapore Management University