An APEC Roadmap for a New Financial Services Data Ecosystem

An Undertaking of the
Asia-Pacific Financial Forum (APFF)

TO IMPLEMENT THE CEBU ACTION PLAN’S INITIATIVE 1A

PROMOTE AN ENABLING FINANCING ENVIRONMENT FOR MSMEs, INCLUDING TRADE, SUPPLY CHAIN AND ALTERNATIVE FINANCING MECHANISMS

DELIVERABLES
PROMOTE THE DEVELOPMENT OF NEW FINANCIAL INSTRUMENTS FOR MSMEs
ADDRESS REGULATORY BARRIERS TO DIGITAL, MOBILE AND INNOVATIVE FINANCING
DEVELOP POLICY FRAMEWORKS FOR ALTERNATIVE FINANCE
# An APEC Roadmap for a New Financial Services Data Ecosystem

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>1. INTRODUCTION</td>
<td>8</td>
</tr>
<tr>
<td>2. GENERAL DATA REGULATION</td>
<td>10</td>
</tr>
<tr>
<td>2.1. Core Principles of Data Protection</td>
<td>10</td>
</tr>
<tr>
<td>2.2. Consistency among Domestic Laws and Regulations</td>
<td>10</td>
</tr>
<tr>
<td>2.3. Expanding the Collection and Sharing of Data</td>
<td>11</td>
</tr>
<tr>
<td>2.3.1. Full-file and comprehensive credit information systems</td>
<td>11</td>
</tr>
<tr>
<td>2.3.2. Uses of unstructured data (Big Data) and industry regulation</td>
<td>15</td>
</tr>
<tr>
<td>2.4. Creating Sound Frameworks for the Collection, Storage, Sharing and Use of Data</td>
<td>16</td>
</tr>
<tr>
<td>2.4.1. Data Protection and Privacy in the Digital Age</td>
<td>16</td>
</tr>
<tr>
<td>2.4.2. Consumer Consent and Use of Personal Data</td>
<td>18</td>
</tr>
<tr>
<td>2.4.3. Use of data and derived data: Rights and responsibilities</td>
<td>20</td>
</tr>
<tr>
<td>2.4.4. Ensuring a Level Playing Field</td>
<td>21</td>
</tr>
<tr>
<td>2.4.5. Ensuring Confidence and Trust in Algorithms</td>
<td>22</td>
</tr>
<tr>
<td>2.4.6. Proposed Actions</td>
<td>23</td>
</tr>
<tr>
<td>3. CROSS-BORDER DATA FLOWS</td>
<td>24</td>
</tr>
<tr>
<td>3.1. Addressing the Concerns Behind Data Localization</td>
<td>24</td>
</tr>
<tr>
<td>3.2. Addressing Cross-Border Data Privacy Protection: Toward an APEC Privacy Regime</td>
<td>26</td>
</tr>
<tr>
<td>3.3. Addressing Data Security Protection</td>
<td>28</td>
</tr>
<tr>
<td>3.4. Facilitating Access to Data for Law Enforcement Purposes</td>
<td>33</td>
</tr>
<tr>
<td>3.5. Promoting the Development of the Domestic Data Infrastructure and Data-Driven and Technology Industries</td>
<td>33</td>
</tr>
<tr>
<td>3.6. Establishing Regional Platforms for Enabling Appropriate Use of New Technologies in Cross-Border Financial Services</td>
<td>35</td>
</tr>
<tr>
<td>4. CONCLUSION</td>
<td>36</td>
</tr>
</tbody>
</table>

APPENDIX: Conference Speakers and Moderators and Conference Call Participants | 38   |
An APEC Roadmap for a New Financial Services Data Ecosystem

EXECUTIVE SUMMARY

There is great potential in harnessing technology and data to achieve greater financial inclusion and efficiency. Actualizing this potential calls for efforts within APEC to develop a shared vision of a trusted and secure future data ecosystem and to collaborate in achieving this. It also 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, the Asia-Pacific Financial Forum (APFF) under the leadership of the APEC Business Advisory Council (ABAC) provided a platform for key stakeholders from the private and public sectors and multilateral and academic institutions to undertake a series of conference calls and conferences/roundtables in Singapore, Washington DC, USA, Atlanta, USA and Beijing, China to create this Roadmap. [See the Appendix for the list of conference call participants and conference speakers.]

This Roadmap identifies critical building blocks of an enabling data ecosystem for the region. It 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. This Roadmap 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. It is hoped that these will enable the expanded collection, sharing and use of data within and across jurisdictions leading to greater inclusiveness and efficiency of financial services in the region.

The following table lists the various elements of the Roadmap and the corresponding proposed actions that economies may consider:

<table>
<thead>
<tr>
<th>Roadmap Element</th>
<th>Proposed Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core principles of data protection as fundamental basis for legislation and regulations around data.</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Consistency among domestic laws and regulations</strong></td>
<td>Economies are encouraged to 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.</td>
</tr>
<tr>
<td></td>
<td>■ To do this, they are encouraged to review those laws, policies and regulations in collaboration with the financial industry, enterprises and consumers, and undertake changes where needed to reinforce agreed upon objectives.</td>
</tr>
<tr>
<td></td>
<td>■ Reforms should be undertaken using a proactive, holistic and systematic approach.</td>
</tr>
<tr>
<td></td>
<td>■ Instead of responding to past challenges, reforms should be as forward-looking as possible based on an adequate analysis</td>
</tr>
</tbody>
</table>
of the technology and industry landscape and trends, as well as scenarios.

| Expanding the collection and sharing of data | Economies are encouraged to 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).

- This requires 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. Where needed, systems may be supplemented by consent-driven processes whereby additional credit information can be collected.
- 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* and other relevant internationally accepted principles, guidelines, standards, good practices and conventions, as appropriate.

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

| Creating sound frameworks for | In addition to alignment on key principles like transparency, open |
Regulators should consider focusing on providing principles while supporting a broader role for industry in developing codes of conduct, market-based standards and self-regulation, and in promoting financial education and public awareness. Regulators and industry should jointly undertake regular reviews of methodologies and algorithms and collaborate in developing robust data standards, best practices in data governance and management and a regulatory environment that fosters innovation.

Policy makers and regulators are encouraged to 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 are best undertaken using a proactive, holistic and systemic approach. Instead of responding to past challenges, reforms 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. It should 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 are encouraged to 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 can develop codes of conduct based on the adopted principles and undertake self-regulation, in coordination with supervisory authorities and under the oversight of regulators. The development of codes of conduct should involve all relevant stakeholders including incumbent financial institutions and new technology-based market players together with major organizations representing users of financial services.

- 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.

The collection, storage, sharing and use of data

data and interoperability, APEC should consider undertaking 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. This will help regulators to effectively engage with data service providers in ensuring their compliance with laws and regulations. It will enable them to make good judgments on the soundness, inclusiveness and fairness of these service providers’ operating models, methodologies and algorithms and provide effective guidance.
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

| Addressing the concerns behind data localization | APEC economies are encouraged to 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. |
| Addressing cross-border data privacy protection and building an APEC privacy regime | APEC can help develop a regional privacy regime by collaborating with the private sector to promote wider participation of interested economies and businesses in the CBPR, including the appointment of accountability agents in all participating economies, lower certification costs, promoting awareness and development of innovative schemes to enable more MSMEs to undergo APEC CBPR certification. APEC should consider establishing a pathfinder initiative of interested member economies to undertake gap analyses of their privacy regimes with the agreed common benchmark (e.g., current or enhanced APEC Privacy Framework) as a basis for identifying measures needed to achieve inter-operability. These gap analyses should involve collaboration among relevant government agencies and regulators, the private sector and international organizations, including the APFF. The APEC Electronic Commerce Working Group’s Data Privacy Subgroup, on behalf of interested APEC economies, is |
encouraged to continue discussing and exploring options for collaboration on privacy and data protection with the European Commission, including seeking recognition of CBPR as a certification mechanism under its system of binding corporate rules (BCRs). Once robust privacy laws are in place, APEC economies are also encouraged to hold talks with the EU to recognize their equivalence with GDPR.

APEC is encouraged to establish a public-private sector task force to develop best practices for promoting RegTech and LegalTech that economies can adopt to assist MSMEs in dealing with the requirements of stricter privacy regimes, develop core data standards to guide MSMEs and design limited safe harbor provisions for economies to adopt, and vetting and identifying privacy enhancing technologies (PETs) that MSMEs can use to pool and share data safely. The task force should work with relevant bodies to disseminate the best practices and core data standards to MSMEs.

| Addressing data security protection | APEC can contribute to promoting a strong data security environment throughout the Asia-Pacific region that can engender trust in wider data flows, by establishing a regional platform for public and private sectors and relevant international organizations, to help developing economies:  
■ identify gaps in adoption of relevant data security standards, including risk-based security standards;  
■ bridge those gaps and promote inter-operability through capacity-building seminars and technical assistance involving experts from industry, government, multilateral institutions and academia;  
■ develop a long-term strategy for strengthening data security in the region;  
■ develop innovative regional initiatives utilizing new technologies to enable wider data flows within and across member economies, especially those that can be used by MSMEs, that satisfy privacy and data security requirements; and  
■ encourage the establishment of computer emergency or security incident response teams (CERTs or CSIRTs) focused on the financial sector where they do not yet exist, involving financial regulators, and promote regional cooperation among them. |
| Facilitating access to data for law enforcement purposes | Governments need to reform the Mutual Legal Assistance Treaty (MLAT) system to streamline the process of providing law enforcement officials cross-border access 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 |
current international agreements for law enforcement authorities to have access to relevant data in each other’s jurisdictions or establishing new ones as needed. Governments should develop partnerships where possible within existing laws to allow for greater coordination and cooperation between the public and private sector.

Promoting the development of domestic data infrastructure and data-driven and technology industries

Member economies can develop domestic data-driven industries by formulating a holistic set of enabling policies and measures based on the APEC Blueprint for Action on Electronic Commerce, and the APEC Best Practices to Create Jobs and Increase Competitiveness. These include undertaking 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.

Establishing regional platforms for enabling appropriate use of new technologies in cross-border financial services

APEC economies are encouraged to 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 framework of shared accountability and responsibility that can guide financial service industry players rapidly adopting technology-based models;
- pooling of scarce human resources who can support policy and regulatory awareness and development, such as in translating principles-based regulations into implementable and practical requirements;
- design of principles-based legislation and regulations;
- establishment of a clear consumer recourse process to support the uses of data analytics and intelligence; and
- (e) coordination among regulators and industry in the region in developing industry codes and standards to complement and support legal and regulatory frameworks.

Economies should consider introducing regulatory sandboxes that both incumbents and new entrants can utilize. These should be coordinated across jurisdictions wherever there is potential to facilitate the development of innovative financial services. They should also build on existing bilateral memoranda of understanding (MOUs) among regulators 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. Economies should look to broaden the MOUs to include multiple participating jurisdictions.
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 decade1 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, such as 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, quick response (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.

However, 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 dataflows, 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.

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

---

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/]

9
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. 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. 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 conferences/roundtables in Singapore, Washington DC, USA, Atlanta, USA and Beijing, China to create this Roadmap. [See the Appendix for the list of conference call participants and conference speakers.]

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.

2. GENERAL DATA REGULATION

2.1. Core Principles of Data Protection

2 These include the 2008 Global Financial Crisis that resulted in a host of legal and regulatory initiatives, the 2013 NSA-WikiLeaks episode and the 2017 Equifax breaches, which 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-Approved 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).
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 Framework⁴ and the proposed update to the OECD Guidelines by the Oxford Internet Institute⁵ 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 Protection⁶ also provide practical and detailed guidance for implementation.

It is widely acknowledged that the principles contained in these documents 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.

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 are encouraged to promote consistency among the variety of domestic laws, policies and

---

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


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.
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. To do this, they should review those laws, policies and regulations in collaboration with the financial industry, enterprises and consumers, and undertake changes where needed to reinforce agreed upon objectives. Reforms should be undertaken using a proactive, holistic and systematic approach. Instead of responding to past challenges, reforms 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. This can 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.

For example, credit scores used in underwriting loans rely in many cases on traditional data, which capture mostly consumers’ transactions with financial institutions. 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 population of credit invisibles in the USA from 60 million to only 5 million people.

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

---


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.

operating credit reporting service providers (CRSPs), which include credit bureaus and credit registries.

Credit information systems have been evolving as technology develops to meet the needs of consumers and small businesses, financial institutions and regulators, with fintech, supertechn and regtech playing important roles in shaping their interactions. However, the landscape today is being revolutionized by the convergence of nearly unlimited amount of data, nearly unlimited space for data storage now available, nearly unlimited computing power and the emergence of a decentralized data system. These factors are exerting pressure on information networks to evolve from centrally authorized to distributed self-governed networks.

This evolution is being further driven by the emergence of alternative data, and most especially the large volume of unstructured data that are coming out of social media. This introduces new policy issues to be debated, such as whether alternative lenders should share their data with credit bureaus and whether holders or analyzers of unstructured data should provide them to credit bureaus if these data are predictive of ability or intention to repay their loans. The policy issues of collecting and sharing alternative data pose questions about the future of the credit reporting industry's traditional role and business model.

Credit information systems are also evolving to fill the demand for cross-border credit information from a growing immigrant population whose credit information is siloed in their home economies, and the needs of many service providers, including insurers, banks, landlords, auto companies and many other businesses to cater to the needs of this market. Such services face various regulatory barriers to cross-border data transfers arising from data localization and limitations on data transfers by sector or type of recipients (e.g. personal credit data, health records, companies not locally registered) and by jurisdiction (e.g., if the receiving jurisdiction does not have adequate data protection regimes). Another critical challenge is ensuring data integrity through the accurate translating of credit information from one market to another into usable data for service providers.

The growing importance being given to consumer protection in various jurisdictions is another feature of the evolving credit information landscape. The increasing sophistication of bad actors is a challenge that regulators are facing, alongside the challenge of ensuring that consumer protection goes hand-in-hand, and not in conflict, with innovation. Aside from domestic efforts such as the use of regulatory sandboxes to meet these challenges, regulators are also increasingly becoming aware of the need for cross-border sharing of experiences and collaboration. The establishment of the Global Financial Innovation Network (GFIN) is a manifestation of this increased awareness.

The rapidly changing credit information landscape requires a review of a number of policy and regulatory issues, including lending safely, privacy, cyber security, fair lending and consumer protection. It requires increased attention to reforming the persistent siloed structure of credit information and consideration of how to deal with new kinds of data and new technology companies that now have control over large amounts of data.

Credit reporting is currently undergoing a paradigm shift. Its traditional focus has been on payment behavior and customer identification and verification, with emphasis on risk management and compelling repayment. It involved a narrow set of reporting institutions, in many instances limited to financial institutions. The new paradigm for information sharing that is emerging is the “financial services data ecosystem.” This new paradigm recognizes the potential to use all types of data on customers not just for risk management but also for sales and customer management. It involves a wide range of potential data providers.

Much remains to be done to address various issues around credit reporting, data sharing and financial inclusion. These include addressing consumer protection issues about discriminatory effects of algorithms, especially with the increasing use of unstructured data in combination with artificial intelligence and machine learning, oversight of data sets that become disintermediated through initiatives like the EU’s second Payment Services Directive (PSD2), regulatory loopholes that platforms can use to avoid penalties for consumer harm, lack of enforcement capacity, and the entry of Big Tech firms with access to large amounts of consumer data in financial services, among others. These concerns reflect the need for flexible, iterative types of regulations and the need for policy makers and regulators to have

13
access to expertise and understand the evolving realities.

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; 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);
- 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, 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 following documents can serve as a reference for economies in developing or improving their frameworks:

- the World Bank’s General Principles for Credit Reporting;¹²

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](https://www.gleif.org/en)

¹³ World Bank, General Principles for Credit Reporting (September 2011)
the International Committee on Credit Reporting (ICCR) Guidance Note on the Use of Alternative Data;  
the G20 High Level Principles for Financial Consumer Protection;  
the 2013 revised edition of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data;  
the Madrid Resolution on International Standard on the Protection of Personal Data and Privacy adopted at the 2009 International Conference on Data Protection and Privacy Commissioners;  
Australia’s Consumer Data Right;  
the 2005 APEC Privacy Framework; and  
the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;  

Proposed action:

Economies are encouraged to 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). This requires 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. Where needed, systems may be supplemented by consent-driven processes whereby additional credit information can be collected. They should collaborate to

14 Key recommendations are as follows:

• Improving the availability and accuracy of information (issuance by regulators and policy makers of guidance on sourcing and processing of alternative data; creation of unique IDs; digitization of public information);
• Expanding credit information sharing (review of regulations to require all financial service providers to report credit data and relevant information to credit reporting service providers (CRSPs); promotion of open, fair and competitive credit information sharing by CRSPs; establish a credit registry or databank to promote information sharing; and establishing oversight);
• Enabling cross-border data exchanges (international policy and regulatory coordination and collaboration through standard setting bodies to develop cross-border data sharing standards and cross-border information regulations; development of protocols for exporting data in the absence of harmonized standards; and identification of core data for financial and commercial purposes);
• Balancing integrity, innovation and competition (agreement on principles of responsible innovation; and supporting innovation through regulatory sandboxes and other programs);
• Data privacy, consumer protection and cyber security (addressing accuracy, integrity, consumer recourse, discrimination); and
• Maintaining pricing transparency (looking at how alternative data contribute to competitive environment).

ICCR, Guidance Note on Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs Operating in the Informal Economy

15 G20 High Level Principles on Financial Consumer Protection (October 2011)  
17 OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)  
18 2009 International Conference on Data Protection and Privacy Commissioners, International Standard on the Protection of Personal Data and Privacy: Madrid Resolution  
19 Consumer Data Right  
20 APEC Privacy Framework (December 2005)  
21 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)
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 and other relevant internationally accepted principles, guidelines, standards, good practices and conventions, 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. However, barriers continue to exist, 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 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 are encouraged to 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 maintaining a comprehensive and dedicated law or an over-arching regulation on personal data protection that reflects this approach. Where needed, they should establish a general personal data regulator that has capacity to implement and power to enforce. The data ecosystem should also include an independent
industry association and practice codes of conduct. It should include efficient and low-cost complaint, correction and dispute resolution mechanisms, particularly out-of-court procedures. It should provide rules governing cross-border data cooperation, investigations and data flows. It should also contain specific financial sector regulations and guidelines for firms providing financial services. As the largest holder of data in the economy, government can 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), unauthorized access is equivalent to theft and serious sanctions are 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 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 sacrosanct 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, virtual assistants, health monitors, drones and satellites, as well as new use cases and business models. Their continued rapid evolution creates concerns about the continued relevance and effectiveness of existing legal and regulatory frameworks in serving the interests of individuals and organizations. These concerns include 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.

There is a certain view that the GDPR may not necessarily be suitable as a model for jurisdictions outside Europe, where innovation that is needed for development and being encouraged by governments and regional organizations like APEC may be stifled. This would be especially relevant for innovations such as the IoT that are heavily reliant on data and have considerable potential. Concerns about the GDPR include its over-reliance on transparency and choice, where consumers are burdened by having to read lengthy privacy policies to protect themselves, its broad-brush approach (e.g., applying same level of protection to health data and other non-sensitive data), its impact on industry competition and concentration (e.g., benefiting large tech companies and large advertisers), and its potential restrictive impact on adoption of technologies like blockchain and artificial intelligence.

However, given that no major alternative model outside Europe yet exists, an increasing number of jurisdictions have introduced or are looking to introduce new laws patterned after the GDPR. The USA is still in the process of addressing its multiplicity of sectoral privacy laws – 27 laws covering various sectors – the existence of gaps in other sectors, and the concern about fragmentation as states enact their own privacy laws, such as those recently passed by state legislatures in California and Vermont. Previously, it was thought that the best way would be to have self-regulation backed by strong enforcement and encouraging its wide adoption, and so there was no serious effort to develop a federal privacy framework.

In light of recent developments, a “new paradigm” is being discussed, centered on the idea that there are uses of data that are considered good (and have been vetted), some that are considered bad,22 and others that should be left to regulators using reasonable parameters that are balanced. Drawing upon the advertising industry’s current self-regulatory principles, federal legislation is being proposed to clearly define data practices that are prohibited while ensuring that consumers continue to benefit from the responsible use of data, with the law backed by enforcement and strict penalties for non-compliance. While such an undertaking still faces the challenge of defining practices in use of data which are different across industries, successfully enacting such a law in the USA may provide an alternative model that APEC member economies can study in further developing their privacy regimes.

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

22 Examples of bad data practices cited are (a) using a person’s data to reject their application or set unfavorable terms of a service, unless specifically permitted by law; (b) using personal characteristics such as race or religion to discriminate in pricing or determining eligibility; (c) sharing data with companies that are known to defraud consumers; (d) collecting sensitive data without the consumer’s permission, subject to limited exceptions; and (e) sharing consumer data with third parties without enforceable contracts to ensure the legal use of these data. Privacy for America: Creating a Strong Paradigm for Privacy and Responsible Data Use (https://www.privacyforamerica.com/wp-content/uploads/2019/04/New-Paradigm-Overview-4-8-19.pdf).
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 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 laws.23

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 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.

23 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.23

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 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 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 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

---

25 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.
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.

Industry can play a key role in promoting trust in AI by promoting the adoption of good practices in its design. Examples are practices founded on the following key pillars:26

---

Fairness: Understanding how bias can be introduced and affect recommendations, employing a diverse group of talent, developing analytical techniques to detect and eliminate bias and incorporating human review based on domain expertise;

Reliability and Safety: Evaluation of training data, extensive testing, monitoring of ongoing performance, designing for unexpected circumstances and including a human being in the loop;

Privacy and Security: Compliance with existing privacy laws, providing transparency on data collection and use with good controls enabling people to make own choices about their data; designing systems to protect against bad actors, and de-identification techniques to promote both privacy and security;

Inclusiveness: Adoption of inclusive design practices to address potential barriers that lead to exclusion, enhancing opportunities for disabled, building trust through contextual interaction; and developing EQ in addition to IQ;

Transparency: Enabling people to understand how decisions were made, providing contextual explanations, and facilitating awareness of potential bias, errors and unintended outcomes; and

Accountability: Holding people accountable for how their systems operate, observing norms during system design and in an ongoing manner, and introducing internal review boards.

Continued innovation and trust in AI will require collaboration between industry and government to develop an ecosystem that includes the following elements:

- a regulatory environment that fosters AI innovation;
- practical principles for trustworthy and human-centered AI;
- voluntary, consensus-driven and market-based standards;
- multi-stakeholder dialogues;
- sharing of best practices;
- data availability;
- modernized social safety net;
- skills training; and
- funded research and development.

2.4.6. Proposed actions:

In addition to alignment on key principles like transparency, open data and interoperability, APEC should consider undertaking 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. This will help regulators to effectively engage with data service providers in ensuring their compliance with laws and regulations. It will enable them to make good judgments on the soundness, inclusiveness and fairness of these service providers’ operating models, methodologies and algorithms and provide effective guidance.

Regulators should consider focusing on providing principles while supporting a broader role for industry in developing codes of conduct, market-based standards and self-regulation, and in promoting financial education and public awareness. Regulators and industry should jointly undertake regular reviews of methodologies and algorithms and collaborate in developing robust data standards, best practices in data governance and management and a regulatory environment that fosters innovation.

Policy makers and regulators are encouraged to 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 are best undertaken using a proactive, holistic and systemic approach. Instead of responding to past challenges, reforms 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. It should 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 are encouraged to 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 can develop codes of conduct based on the adopted principles and undertake self-regulation, in coordination with supervisory authorities and under the oversight of regulators. The development of codes of conduct should involve all relevant stakeholders including incumbent financial institutions and new technology-based market players together with major organizations representing users of financial services.

- 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.

3. CROSS-BORDER DATA FLOWS

The cross-border flow of data is an important issue for Asia-Pacific economies, as their continued prosperity depends on 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 on 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. National security is sometimes mentioned as

---

27 Alignment with OECD principles require organizations also respect the collection limitation principle (irrespective of misuse).


a driver, although as it is already well-recognized as a legitimate reason for making exceptions to cross-border data 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.” 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 by the European Centre for International Political Economy (ECIPE) pointed to substantial negative impact of enacted or proposed data localization legislation on seven major economies (average of -0.7 percent of GDP in these economies). 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, 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 their ability 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.

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 are encouraged to 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.

ows-in-asia/}


3.2. Addressing cross-border data privacy protection: Toward an APEC Privacy Regime

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.

APEC officials have for many years been undertaking various efforts to address concerns about privacy in order to ensure trust in continued cross-border data flows, which are critical to achieving APEC’s goal of free and open trade and investment. Member economies agreed on an APEC Privacy Framework oriented toward promoting economic growth (in contrast to the EU’s GDPR, which focused on protecting consumers’ fundamental rights). Key characteristics of the Framework include a balance between privacy protection and need for data flows, flexibility in implementation based on promoting consistency rather than harmonization, encouragement of cross-border data transfers and inter-operability and a risk-based and proportionate approach to the regulation of data flows.

Building on the APEC Privacy Framework, member economies established the Cross-Border Privacy Rules (CBPR) as the mechanism for enabling companies to share data across borders while protecting privacy. The economies that have agreed to participate in the CBPR (9 economies as of March 2019) together account for a total population of 830 million, a combined GDP of USD32.5 trillion or 27.2% of the world total, and a 26.1% share in total world exports, figures that are in all corresponding cases higher than those for the EU. The CBPR, however, is still at a very early stage of development, and is currently endeavoring to broaden its reach, create momentum and uptake and ensure global inter-operability. It has gained support from many member economies and recognition in the US-Mexico-Canada Agreement (USMCA). Japan has taken an active role in promoting data flows with trust. Five economies have made commitments in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) that align with CBPR adoption. There is also potential for further expansion through the Pacific Alliance. Within the next several months, several more economies and accountability agents are expected to join.

The CBPR shares with the GDPR a common point of origin, which is the OECD Privacy Guidelines. However, there are significant differences in approaches between the two regimes. The GDPR, on one hand, is explicit in defining the fundamental individual right to privacy as its basis, a legal framework applying to sectors and EU member states, aiming to facilitate a Digital Single Market and has specific articles on cross-border data transfers and extraterritorial enforcement. The CBPR on the other hand, is guided by APEC member economies’ implicit references to privacy rights, based on self-regulation and coordination rather than a common legal framework, and depends on companies’ perceptions of benefits for attracting participation. Both, however, recognize the need for a risk-based, balanced and flexible approach. While there are clear divergences between these two regimes at present, there remains scope for achieving future inter-operability.

The GDPR provides three ways for inter-operability (i.e., allowing personal data to be shared) with other jurisdictions: (a) when the Commission decides that the other jurisdiction provides the same level of protection as in the EU (adequacy); (b) when certain derogations apply; and (c) when there are appropriate safeguards such as standard contractual clauses, approved codes of conduct, approved certification mechanisms, and binding corporate rules (BCRs).

Many jurisdictions are introducing new privacy legislation and rules based on their own reviews of provisions in the GDPR. However, they face various challenges to achieving adequacy. A number of jurisdictions are adopting rules from the GDPR that they view are applicable to their respective situation while precluding those they view as not in line with business models in their markets, cross-border trade, state of technological advancement, social and political values and legal systems. There are differences in terminology and definitions, such as for example the definition of personal information and sensitive data (which is not defined in some economies’ data protection laws). Jurisdictions will also need to decide
whether they wish to adopt certain GDPR articles that can entail significant operational costs for businesses, such as requirements to hire particular personnel, acquire new technologies and obtain legal advice.

The CBPR system is envisaged to allow companies in APEC to apply for certification under the EU system of BCRs, if the CBPR is recognized by the EU as a certification mechanism under the GDPR. While there is some unofficial acknowledgement by individual EU officials that CBPR is equivalent to GDPR, inter-operability has yet to be agreed. A comparison of rules under CBPR and GDPR\(^3\) shows partial alignment but also significant divergence. Following are several areas of divergence:

- The GDPR principle of “storage limitation” (which requires that personal data should not be retained longer than necessary, in relation to the purpose for which it is being processed) has no equivalent in CBPR.
- Notification of data breach (to implement the principle of “preventing harm”) is mandatory under GDPR but is only encouraged and not mandated under CBPR.
- Onward transfer (transfer to a third country or international organization) of personal data is subject to adequacy decisions, appropriate safeguards or derogations under GDPR but is not mentioned in CBPR.
- Cross-border transfer of personal data is subject to adequacy decisions, appropriate safeguards or derogations under GDPR. Under CBPR it is allowed if sufficient safeguards are in place. The CBPR also applies restrictions in a manner proportionate to risks.

An important issue that needs to be addressed is the low level of participation in CBPR. There are currently 8 participating economies,\(^2\) with several more expected to join. There are only 27 companies (24 US and 3 Japanese, not including subsidiaries) that have joined. There are only 2 accountability agents – one in the USA and another in Japan, although efforts are under way to recruit several more. The relatively high cost of certification of compliance with the APEC Privacy Framework relative to perceived commercial benefits among many companies are serious barriers to wider participation in the scheme. To date, several companies have indicated that their main reason for joining CBPR is to enhance their reputation rather than to obtain commercial benefits from cross-border data transfers. The success of CBPR will hinge on how these issues can be addressed to attract a critical mass of companies in many APEC economies, including SMEs, to participate.

The critical issue in the cross-border sharing of personal information is trust in the effectiveness of mechanisms to prevent the disclosure of individuals’ personal information without their consent. The CBPR provides a pathway for engendering trust in participating companies’ ability to meet this requirement, and is an already existing mechanism, albeit at a very early stage, that can be further developed. However, the long-term solution lies in the inter-operability of legal frameworks governing privacy among APEC member jurisdictions, through the development of an Asia-Pacific regional privacy regime. Given the wide diversity of APEC member economies including their legal traditions, significant variations in their privacy laws are to be expected, which will pose challenges to achieving inter-operability.

Developing a regional privacy regime will require incremental steps that will involve efforts by member jurisdictions to agree on a common benchmark, such as the APEC Privacy Framework,\(^3\) introduce or develop privacy laws aligned with the benchmark, identify specific provisions that need to be harmonized and derogations (exemptions from certain provisions) that can be applied, and undertaking needed legislative actions. Given the voluntary nature of APEC and that not all economies may be ready to join the process at the start, such an initiative may have to be undertaken on a pathfinder basis.

\(^{11}\) Maria Vasquez Callo-Müller, GDPR and CBPR: Reconciling Personal Data Protection and Trade [APEC Policy Support Unit Policy Brief No. 23, October 2018].

\(^{22}\) As of March 2019, these are: USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia and Chinese Taipei.

\(^{33}\) The APEC Privacy Framework could be used as a benchmark by itself or enhanced by various techniques of legal harmonization such as model law, legislative guides and recommendations, model provisions (e.g., for the APEC Privacy Framework), contractual techniques (standardization of clauses or rules), and legal guides (providing explanations on drafting of laws).
Inter-operability with GDPR can be pursued in the short and medium term through negotiations leading to the recognition of CBPR by the EU as a certification mechanism under its system of binding corporate rules (BCRs), and over the long term through talks with the EU to recognize the equivalence of privacy laws in APEC jurisdictions with GDPR.

Another issue that requires immediate attention is how to help MSMEs, which have insufficient resources to deal with the growing complexity of the global privacy landscape that can impede their ability to operate in cross-border digital environments. There are several measures that can be considered. One is the promotion of technologies facilitating regulatory compliance (RegTech) and those facilitating contracts and litigation (LegalTech). Another is public-private collaboration to develop core data standards that can serve as a guide for MSMEs and providing limited safe harbor (statutory or regulatory provisions exempting certain conduct from compliance) for those MSMEs that comply. A third possible measure is the vetting and identification of privacy enhancing technologies (PETs) that MSMEs can use to pool and share data safely, such as differential privacy that limits access of users to summaries of data (e.g., averages) and introduces noise into these summaries.

**Proposed actions:**

- APEC can help develop a regional privacy regime by collaborating with the private sector to promote wider participation of interested economies and businesses in the CBPR, including the appointment of accountability agents in all participating economies, lower certification costs, promoting awareness and development of innovative schemes to enable more MSMEs to undergo APEC CBPR certification.
- APEC should consider establishing a pathfinder initiative of interested member economies to undertake gap analyses of their privacy regimes with the agreed common benchmark (e.g., current or enhanced APEC Privacy Framework) as a basis for identifying measures needed to achieve inter-operability. These gap analyses should involve collaboration among relevant government agencies and regulators, the private sector and international organizations, including the APFF.
- The APEC Electronic Commerce Working Group’s Data Privacy Subgroup, on behalf of interested APEC economies, is encouraged to continue discussing and exploring options for collaboration on privacy and data protection with the European Commission, including seeking recognition of CBPR as a certification mechanism under its system of binding corporate rules (BCRs). Once robust privacy laws are in place, APEC economies are also encouraged to hold talks with the EU to recognize their equivalence with GDPR.
- APEC is encouraged to establish a public-private sector task force to develop best practices for promoting RegTech and LegalTech that economies can adopt to assist MSMEs in dealing with the requirements of stricter privacy regimes, develop core data standards to guide MSMEs and design limited safe harbor provisions for economies to adopt, and vetting and identifying privacy enhancing technologies (PETs) that MSMEs can use to pool and share data safely. The task force should work with relevant bodies to disseminate the best practices and core data standards to MSMEs.

### 3.3. Addressing Data Security Protection

#### 3.3.1. Responding to the Growing Threats to Data Security

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. This is reflected in various initiatives promoted by the private sector, as well as international and public-private collaboration.

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;
- A common lexicon of cybersecurity terminology to facilitate communication and improve international collaboration, as well as to promote legal harmonization;
- Public-private collaboration to develop policies for coordinated vulnerability disclosure in systems and hardware;
- Guidelines for sharing of data security threat information among governments, industry and other relevant stakeholders based on established international standards to promote higher levels of

---

35 For example, the US Chamber of Commerce established a cyber working group to look at relevant legislation and to promote international inter-operability with the USA’s major economic partners. Currently, the Chamber is looking for opportunities to promote the framework in the Asia-Pacific region, where many governments are also looking for frameworks around critical infrastructure. Core pieces of legislation under the framework include (a) risk management and security measures; (b) measures for firms to report on cyber incidents; and (c) penalties and sanctions for non-compliance. Other relevant initiatives of the Chamber include the development of a model cyber security law and cyber incident reporting framework.

36 These include arrangements such as the Asia-Pacific Computer Emergency Response Team (APCERT), ASEAN CERT and the ASEAN Cyber Capacity Program (ACCP), as well as the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) to develop norms.
mutual trust and enable wider intelligence-sharing among jurisdictions to facilitate emergency responses;

- Innovative programs for security in payments and other industries that are 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 exchange of experiences, expertise and strategies to improve information and communication infrastructure, develop skills and advise on policies.

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,37 public key infrastructure (PKI),38 encryption of data at rest and in transit,39 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.

Cyber insurance could also be used to strengthen data security.40 Such arrangements could stimulate the adoption of best practices through insurance requirements and, if properly designed, create incentives for participating in programs that reduce risk for all those connected to the Internet. However, for cyber insurance to work, several challenges need to be addressed. Challenges for insurers include lack of data due to underreporting of incidents or the early stage of development of the market (without which insurers are unable to sufficiently develop predictive models and evaluate probabilities of loss); constant threat mutation due to the rapid pace of innovation and development and deployment of new tactics by cyber criminals; and catastrophic events that could lead to a flood of claims.

Challenges for buyers include the difficulty of understanding risks and market; lack of standard policy language in the insurance industry; legal uncertainty (lawsuits over disputed claims have not yet been brought to court; and unsuitable policy terms (e.g., when lumped together with other provisions like property, crime and general liability). Overcoming such challenges may entail insurers temporarily switching from a predictive to a risk-based model until enough data is gathered and translated into policies; redesign of cyber insurance to encompass a buyer’s cyber risk life cycle and standardization of terminology among insurers; and insurers conducting risk awareness campaigns.

Data governance and management are central to resolving existing concerns around the free flow of data across borders, as well as in the sharing, storage and use of data within a jurisdiction. 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

---

37 Public-key cryptography (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).

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

39 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).

40 In the USA, one proposal involved the legislature putting in place a federal backstop for cyber insurance to cover catastrophic events in cyber space, patterned after similar arrangements used to repair the damage from catastrophes like hurricanes and prevent incidents from recurring. Such a backstop could be established by expanding the existing Terrorism Risk Insurance Program (TRIP) (which enables the federal government to reimburse a portion of insurance companies’ costs if the losses exceed the insurer’s deductible and are caused by a certified act of terrorism) to also cover all cyber attacks, regardless of their source. Companies would be required to purchase a minimum level of insurance and will be obliged to implement a cyber security plan modeled on NIST’s cyber security framework, participate in the Automated Indicator Sharing (AIS) program and submit to comprehensive investigations after cyber incidents. Robert K. Knake, “Creating a federally sponsored cyber insurance program,” CFR, November 2016.
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.

3.3.2. Developing a Regional Framework for Industry-Government Collaboration in Data Security

Increasing amounts of data are being used in financial services, especially as financial institutions progressively adopt machine learning and artificial intelligence to improve capabilities to analyze, streamline and automate business lines. This applies especially to credit risk management and anti-money laundering. Financial institutions face various constraints in the use of data, both internal (e.g., legacy IT systems) and regulatory (e.g., data privacy and localization requirements) but are also making improvements to be able to take advantage of opportunities in using data. More and more financial institutions are also under pressure to move data to the cloud. This pressure is coming from clients, from regulators and from competition with new big players.

As digitalization progresses, the need for a new digital infrastructure that is secure, smart and able to protect privacy becomes increasingly important for businesses and consumers to move away from paper documents to digital documents, especially in cross-border transactions. Efforts to build such new infrastructure have generated benefits such as government savings, fraud reduction and increased tax base, but the process involves huge upfront investment and long-term infrastructure build-up. However these government-led initiatives have not been successful in promoting industry participation due to weaknesses in privacy and data security protection. Blockchain offers an opportunity for an industry-initiated and government-supported initiative that could allow for more secure flow of data among businesses, government agencies and individuals. Data could be cross-verified within jurisdictions through the use of AI.

The development of a secure cross-border data ecosystem requires participation of both government and industry, with government designing principles and broad guidelines and the industry taking a more active role by developing codes of conduct and establishing self-regulatory mechanisms supported by regulatory authorities. Industry self-regulation with the collaboration of regulatory authorities can provide a more agile framework for promoting data security in the region.

Effective adoption of relevant internationally recognized standards, as appropriate for each economy, is critical to the maintenance of a robust data security environment. Such international standards may include those governing the preservation of confidentiality, integrity and availability of data (both in

41 Examples are Estonia’s X-Road and India’s Aadhaar.

42 Blockchain is already being used to exchange information across borders, such as in the case of the Interbank Information Network (IIN) (launched by J.P. Morgan in 2017 and joined since then by already more than 200 banks), which enables banks to exchange information in real-time as a way to verify that a payment has been approved. In Latin America, Proyecto Cadena was launched to enable Customs administrations, which engage in a Mutual Recognition Agreement, to share a single view of the status of an Authorized Economic Operator certificate in real time while ensuring that the highest standards of security, traceability, and confidentiality are applied to the data. This replaces the previous system, where designated Customs officers in each administration send, by email, an Excel file containing the data elements that the countries agreed to exchange on their respective AEOS.

43 The US National Institute of Standards and Technology (NIST) under the US Department of Commerce follows the Cybersecurity Framework based on ISO/IEC standards. The NIST framework adopts the five functions of the ISO/IEC 27001 Information Security Management System for implementing risk-based approach to cybersecurity: (a) Identify (understand risks), (b) protect (determine safeguards); (c) detect (identifying events); (d) respond (address incidents) and (e) recover (restore capabilities). Although not universally adopted, the NIST framework is broadly applicable, including to SMEs, and is a good starting point for thinking about data security.
physical and electronic form), such as those set out in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002, the other ISO/IEC 27000-series standards, and relevant cybersecurity standards, among others, such as:
- the European Telecommunications Standards Institute (ETSI) Cyber Security Technical Committee (TC CYBER) standards,
- ISO/IEC 21827 governing organizations’ security engineering processes,
- the Information Security Forum (ISF) Standard of Good Practices (SoGP) on management of information security risks in business organizations and their supply chains,
- the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF),
- ISO 15408 governing the integration and testing of software and hardware products,
- the Internet Engineering Task Force (IETF) Site Security Handbook RFC 2196 providing a guide to setting computer security policies and procedures for sites that have systems on the Internet,
- the IEC 62443 standards listing cybersecurity protection methods and techniques, and
- the Information Assurance for Small and Medium Enterprises (IASME) Governance standard for cybersecurity and protection of customer information in MSMEs participating in supply chains.

Of particular importance is the strengthening of encryption and cryptography standards addressing algorithms, applications and related security considerations for successful implementation. These include relevant standards under ISO/IEC, American National Standards Institute (ANSI)/Society of Cable and Telecommunications Engineers, and the Institute of Electrical and Electronics Engineers (IEEE).

**Proposed actions:**

- APEC can contribute to promoting a strong data security environment throughout the Asia-Pacific region that can engender trust in wider data flows, by establishing a regional platform for public and private sectors and relevant international organizations, to help developing economies (a) identify gaps in adoption of relevant data security standards, including risk-based security standards; (b) bridge those gaps and promote inter-operability through capacity-building seminars and technical assistance involving experts from industry, government, multilateral institutions and academia; (c) develop a long-term strategy for strengthening data security in the region; (d) develop innovative regional initiatives utilizing new technologies to enable wider data flows within and across member economies, especially those that can be used by MSMEs, that satisfy privacy and data security requirements; and (e) encourage the establishment of computer emergency or security incident response teams (CERTs or CSIRTs) focused on the financial sector where they do not yet exist, involving financial regulators, and promote regional cooperation among them.

### 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 need to reform the Mutual Legal Assistance Treaty (MLAT) system to streamline the process of providing law enforcement officials cross-border access 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 current international agreements for law enforcement authorities to have access to relevant data in each other’s jurisdictions or establishing new ones as needed. 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.44

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

---

44 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.
entrant 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.

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 can develop domestic data-driven industries by formulating a holistic set of enabling policies and measures based on the APEC Blueprint for Action on Electronic Commerce, and the APEC Best Practices to Create Jobs and Increase Competitiveness. These include undertaking 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.

### 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

---

45 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]

46 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].
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 no longer being relevant or effective by the time they are put in place. Another related challenge is the 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 an initiative 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 through its APIX platform. AFIN 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 in certain economies 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 existing, as well as planned, sandboxes in APEC economies.

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 are encouraged to 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 rapidly adopting technology-based models; (b) pooling of 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) 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 (e) coordination among regulators and industry in the region in developing industry codes and standards to complement and support legal and regulatory frameworks.

- Economies should consider introducing regulatory sandboxes that both incumbents and new entrants can utilize. These should be coordinated across jurisdictions wherever there is potential to facilitate the development of innovative financial services. They should also build on existing bilateral memoranda of understanding (MOUs) among regulators 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. Economies should
look to broaden the MOUs to include multiple participating jurisdictions.

4. CONCLUSION

The success of the Asia-Pacific region in achieving its goal of prosperity in the 21st century hinges on its ability to leverage new technologies in the digital economy. In this process, economies’ ability to harness data will be critical, and particularly more so in financial services. There is huge potential in using data to overcome the challenges of accessing finance that face many MSMEs and consumers, particularly in emerging markets. Expanded collection, sharing and use of data have been enablers of financial inclusion, and the current data revolution driven by the rapidly growing volume, variety and velocity of data offers an opportunity to actualize this potential.

Expanded cross-border flow of data is also critical for the realization and success of APEC’s vision of free and open trade and investment, as well as other regional free trade and economic integration ambitions involving member economies such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Regional Comprehensive Economic Partnership (RCEP), the ASEAN Economic Community and the Pacific Alliance. The economic realities of the 21st century will need legal and regulatory frameworks, market conventions and practices that will be different from currently existing ones that are still largely geared toward domestic transactions.

This Roadmap seeks to provide ideas on a way forward for economies in creating an enabling ecosystem for the wider collection, sharing and use of data for the purpose of promoting inclusive and efficient financial services. It also proposes practical steps that economies individually and APEC can take to begin creating a regional regime that can facilitate expanded cross-border data flows by addressing their implications on data security and privacy, law enforcement and development of data infrastructure and data-driven industries.

In the process of developing this Roadmap, the APFF has also given shape to a regional network of experts from public, private, international and academic institutions that are committed to contribute to the development of a new financial services data ecosystem in the region. The APFF invites APEC Finance Ministers to support the use of this Roadmap by relevant authorities and stakeholders in the region to advance the development of this ecosystem and to encourage them to collaborate with the APFF network of experts in implementing the actions proposed.
Conference Calls:
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

1st APFF Data Ecosystem Conference: Charting a Roadmap Toward a New Data Regime for the Digital Economy
June 20-21, 2018, Mochtar Riady Auditorium, Singapore Management University

2nd APFF Data Ecosystem Conference: Building an Asia-Pacific Data Regime for Financial Services: Challenges and Prospects
September 26-27, 2018, Venable Law Offices, Washington DC, USA

Expert Roundtable on an APEC Data Ecosystem for Financial Services: Addressing Security and Privacy Challenges to Facilitate Regional Cross-Border Data Flows
March 2, 2019, The Whitley Hotel, Atlanta, Georgia, USA

3rd APFF Data Ecosystem Conference: Developing Data Protection Legislation and Regulatory Structures
June 14, 2019, Guanghua School of Management, Peking University, Beijing, China

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Position</th>
<th>Conference Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexis Serfaty</td>
<td>Access Partnership Ltd</td>
<td>Director, Global Public Policy</td>
<td>1</td>
</tr>
<tr>
<td>Allan Bollard</td>
<td>APEC Secretariat</td>
<td>Executive Director</td>
<td>2</td>
</tr>
<tr>
<td>Donna McPartland</td>
<td>Arent Fox LLP</td>
<td>Counsel</td>
<td>3</td>
</tr>
<tr>
<td>Lawrence Low</td>
<td>Allen &amp; Gledhill Regulatory &amp; Compliance Pte Ltd</td>
<td>CEO</td>
<td>4</td>
</tr>
<tr>
<td>Raymond Li</td>
<td>Ant Financial Services Group</td>
<td>General Manager, Legal and Compliance Department</td>
<td>5</td>
</tr>
<tr>
<td>May-Ann Lim</td>
<td>Asia Cloud Computing Association</td>
<td>Executive Director</td>
<td>1</td>
</tr>
<tr>
<td>Michael Mudd</td>
<td>Asia Policy Partners LLC</td>
<td>Managing Partner</td>
<td>2</td>
</tr>
<tr>
<td>Peter Tierney</td>
<td>AxiomSL</td>
<td>CEO, APAC</td>
<td>3</td>
</tr>
<tr>
<td>Tod Burwell</td>
<td>BAFT</td>
<td>President and CEO</td>
<td>4</td>
</tr>
<tr>
<td>John Ott</td>
<td>Bain &amp; Co.</td>
<td>Partner</td>
<td>5</td>
</tr>
<tr>
<td>Ksenia Oshmankevich</td>
<td>Bank of Russia</td>
<td>Leading Engineer</td>
<td>1</td>
</tr>
<tr>
<td>Thomas Clark</td>
<td>BlackRock</td>
<td>Managing Director</td>
<td>2</td>
</tr>
<tr>
<td>Paul Watkins</td>
<td>Bureau for Consumer Financial Protection, USA</td>
<td>Director, Office of Innovation</td>
<td>3</td>
</tr>
<tr>
<td>Peter Sheerin</td>
<td>Business Information Industry Association (BIIA)</td>
<td>Committee Chair, Asia-Pacific Consumer Credit Information</td>
<td>4</td>
</tr>
<tr>
<td>Robert Holleyman</td>
<td>C&amp;M International</td>
<td>President &amp; CEO</td>
<td>5</td>
</tr>
<tr>
<td>Ken Katayama</td>
<td>Center for Financial Industry Information Systems, Japan</td>
<td>Director of International Industry Information Systems</td>
<td>1</td>
</tr>
<tr>
<td>Peter Douglas</td>
<td>Chartered Alternative Investment Analyst Foundation</td>
<td>Director</td>
<td>2</td>
</tr>
<tr>
<td>Zeming Yan</td>
<td>China Ministry of Public Security</td>
<td>Chief of Electronic Identity Technology Department</td>
<td>3</td>
</tr>
<tr>
<td>Ping Liu</td>
<td>China State Council</td>
<td>Director General, Finance Research Center</td>
<td>4</td>
</tr>
<tr>
<td>Aijun Li</td>
<td>China University of Political Science and Law</td>
<td>Director, Internet Finance Law Research Institute</td>
<td>5</td>
</tr>
<tr>
<td>Catherine Simmons</td>
<td>Citi</td>
<td>Managing Director and Head of Government Affairs</td>
<td>1</td>
</tr>
<tr>
<td>James Bond</td>
<td>Citi</td>
<td>Head of Government Affairs, Australia</td>
<td>2</td>
</tr>
<tr>
<td>Kimberley Claman</td>
<td>Citi</td>
<td>Director, International</td>
<td>3</td>
</tr>
<tr>
<td>Name</td>
<td>Company/Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stuart Pratt</td>
<td>CoreLogic, Global Head, Public Policy and Industry Relations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dara Dugay</td>
<td>Credit Builders Alliance, Executive Director</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ning Tang</td>
<td>CreditEase, Founder and CEO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chee Kin Lam</td>
<td>DBS Bank Ltd, Managing Director &amp; Head, Group Legal, Compliance &amp; Secretariat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piyush Gupta</td>
<td>DBS Group, CEO and Director</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jean-Remi Lopez</td>
<td>DTCC, Director of Government Relations - Asia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oliver Williams</td>
<td>DTCC Data Repository Services Singapore, CEO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catherine Khaw</td>
<td>Data &amp; Analytics Capital, Founder and Chief Intelligence Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peter Leonard</td>
<td>Data Synergies, Principal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jianmin Zhang</td>
<td>Dentons, Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carolyn Bigg</td>
<td>DLA Piper (Hong Kong), Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boon-Hiong Chan</td>
<td>Deutsche Bank, Director and Head – Market Advocacy APAC/MENA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wijaya Abori</td>
<td>Deutsche Bank, Regional Data Privacy Officer, APAC and Senior Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charmian Aw</td>
<td>Drew &amp; Napier LLC, Director, Telecommunications, Media and Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poh Lip Hang</td>
<td>Drew &amp; Napier LLC, Assistant Head, Competition &amp; Regulatory Economics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tju Liang Chua</td>
<td>Ethereum Foundation, General Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Francis Gross</td>
<td>European Central Bank (ECB), Senior Adviser, Directorate General Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anthony Hadley</td>
<td>Experian, Vice President, International Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mike Pecen</td>
<td>Experian Consumer Information Services, North America, Head of Data Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hongyu Sun</td>
<td>F-Road, Chairman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juan Paolo Fajardo</td>
<td>Fajardo Law Offices, Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>George Shand</td>
<td>FICO Scores, Senior Director, Americas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Umang Moondra</td>
<td>Fidor, APAC Head</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Melissa Koide</td>
<td>FinReg Lab, CEO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clare Sullivan</td>
<td>Georgetown University, Professor, Law Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maryam Cope</td>
<td>GoldsteinCope Policy Solutions, Managing Partner, Technology Practice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toshiki Yano</td>
<td>Google, Head of Privacy and Security, APAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eugenio Briales Gomez</td>
<td>Harvard Law School, Visiting Professor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tarragona</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>William Hallatt</td>
<td>Herbert Smith Freehills, Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Michael Geoffroy</td>
<td>HSBC Bank USA, N.A., Senior Vice President, Office of Public Affairs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jinchang Lai</td>
<td>IFC/World Bank Group, Principal Operations Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gordon Myers</td>
<td>IFC/World Bank Group, Chief Counsel, Technology and Private Equity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hung Ngovandan</td>
<td>IFC/World Bank Group, Principal Financial Specialist</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Randall Riopelle</td>
<td>IFC/World Bank Group, Country Manager for China, Mongolia and Korea</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luz Maria Salamina</td>
<td>IFC/World Bank Group, Lead Financial Sector Specialist</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brad Carr</td>
<td>Institute of International Finance, Senior Director, Digital Finance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conan French</td>
<td>Institute of International Finance, Senior Advisor, Digital Finance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rishi Kapoor</td>
<td>ISDA, Director, Policy, Asia-Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zhijian Liu</td>
<td>JD Finance, General Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Current Position and Organization</td>
<td>Position/Role</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Xijun Liu</td>
<td>Jingdong Digital Technology Holdings Co Ltd</td>
<td>Legal Director, Legal Compliance Department</td>
<td></td>
</tr>
<tr>
<td>Hoon Choi</td>
<td>Korea Financial Services Commission</td>
<td>Director General, Policy Bureau</td>
<td></td>
</tr>
<tr>
<td>Gerard George</td>
<td>Lee Kong Chian School of Business, SMU</td>
<td>Dean/Professor of Innovation and Entrepreneurship</td>
<td></td>
</tr>
<tr>
<td>Yi Lin Sang</td>
<td>Mastercard</td>
<td>Senior Managing Counsel</td>
<td></td>
</tr>
<tr>
<td>Yan Li</td>
<td>Meituan &amp; Dianping Law &amp; Policy Research Institute</td>
<td>Senior Research Fellow</td>
<td></td>
</tr>
<tr>
<td>Carolyn Nguyen</td>
<td>Microsoft Corporation</td>
<td>Director, Technology Policy</td>
<td></td>
</tr>
<tr>
<td>Julius Caesar Parreñas</td>
<td>Mizuho</td>
<td>Senior Advisor</td>
<td></td>
</tr>
<tr>
<td>David Hardoon</td>
<td>Monetary Authority of Singapore</td>
<td>Chief Data Officer</td>
<td></td>
</tr>
<tr>
<td>Brian Yeoh</td>
<td>Monetary Authority of Singapore</td>
<td>Deputy Director, Data Governance &amp; Architecture</td>
<td></td>
</tr>
<tr>
<td>Surapol Opassation</td>
<td>National Credit Bureau Co Ltd</td>
<td>CEO</td>
<td></td>
</tr>
<tr>
<td>Matt Barrett</td>
<td>National Institute of Standards and Technology, USA</td>
<td>Program Manager, NIST Cybersecurity Framework</td>
<td></td>
</tr>
<tr>
<td>Marija Zivanovic-Smith</td>
<td>NCR</td>
<td>Vice President, Communications and Public Affairs</td>
<td></td>
</tr>
<tr>
<td>Makoto Yokozawa</td>
<td>Nomura Research Institute</td>
<td>Visiting Professor, NRI-Kyoto University Joint Research Unit</td>
<td></td>
</tr>
<tr>
<td>Yichen Feng</td>
<td>Nova Credit</td>
<td>Head of Asia Partnership</td>
<td></td>
</tr>
<tr>
<td>Damira Khatam</td>
<td>Nova Credit</td>
<td>Privacy Counsel</td>
<td></td>
</tr>
<tr>
<td>Donald MacDonald</td>
<td>OCBC Bank</td>
<td>Head, Group Customer Analytics &amp; Decisioning</td>
<td></td>
</tr>
<tr>
<td>Dorothy Hill</td>
<td>Pallas Global Advisors LLC</td>
<td>Global Consultant</td>
<td></td>
</tr>
<tr>
<td>Phoram Mehta</td>
<td>PayPal</td>
<td>Head of Information Security</td>
<td></td>
</tr>
<tr>
<td>Huaxiang Ma</td>
<td>Peking University, Guanghua School of Management</td>
<td>Party Secretary and Professor</td>
<td></td>
</tr>
<tr>
<td>Hanson Wang</td>
<td>Peking University, Guanghua School of Management</td>
<td>Director, Business Intelligence Research Center</td>
<td></td>
</tr>
<tr>
<td>Zhicheng Wang</td>
<td>Peking University, Guanghua School of Management</td>
<td>Director, Credit Data Analysis and Application Laboratory</td>
<td></td>
</tr>
<tr>
<td>Shaohua Zhang</td>
<td>Peoples Bank of China</td>
<td>Deputy Director General, Senior Advisors Office</td>
<td></td>
</tr>
<tr>
<td>Gloria Pasadilla</td>
<td>Policy Support Unit, APEC</td>
<td>Senior Analyst</td>
<td></td>
</tr>
<tr>
<td>Kazumi Moore</td>
<td>Policy and Economic Research Council (PERC)</td>
<td>Economic Policy Research Manager</td>
<td></td>
</tr>
<tr>
<td>Michael Turner</td>
<td>Policy and Economic Research Council (PERC)</td>
<td>President</td>
<td></td>
</tr>
<tr>
<td>Patrick Walker</td>
<td>Policy and Economic Research Council (PERC)</td>
<td>Director of Research</td>
<td></td>
</tr>
<tr>
<td>Carl Wegner</td>
<td>R3</td>
<td>Managing Director and Head of Asia</td>
<td></td>
</tr>
<tr>
<td>Luther Moncrief</td>
<td>SAP Asia</td>
<td>Solution Adviser Expert, Database &amp; Data Mgt.</td>
<td></td>
</tr>
<tr>
<td>Duoji Xu</td>
<td>Shanghai Advanced Institute of Finance</td>
<td>Professor</td>
<td></td>
</tr>
<tr>
<td>Ekkehart Boehmer</td>
<td>Sim Kee Boon Institute for Financial Economics, SMU</td>
<td>Academic Director</td>
<td></td>
</tr>
<tr>
<td>Matthew Gamser</td>
<td>SME Finance Forum / IFC</td>
<td>CEO</td>
<td></td>
</tr>
<tr>
<td>Shameek Kundu</td>
<td>Standard Chartered Bank</td>
<td>Chief Data Officer</td>
<td></td>
</tr>
<tr>
<td>Alexander Helfter</td>
<td>Stradegi Consulting</td>
<td>Senior Business Consultant</td>
<td></td>
</tr>
<tr>
<td>Lisa O'Connor</td>
<td>SWIFT</td>
<td>Head of Standards, APAC</td>
<td></td>
</tr>
<tr>
<td>Jianshu Wang</td>
<td>Swiss Re Asia Pte Ltd</td>
<td>Senior Analytics Specialist</td>
<td></td>
</tr>
<tr>
<td>Kobsak Duangdee</td>
<td>Thai Bankers Association</td>
<td>Secretary General</td>
<td></td>
</tr>
<tr>
<td>Peter Lovelock</td>
<td>TRPC Pte. Ltd.</td>
<td>Director and Founder</td>
<td></td>
</tr>
<tr>
<td>Laura Winwood</td>
<td>TRPC Pte. Ltd.</td>
<td>Director</td>
<td></td>
</tr>
<tr>
<td>Shaundra Watson</td>
<td>The Software Alliance</td>
<td>Director, Policy, BSA</td>
<td></td>
</tr>
<tr>
<td>Douglas Amer</td>
<td>The University of Hong Kong</td>
<td>Kerry Holdings Professor in Law</td>
<td></td>
</tr>
<tr>
<td>Daniel Warelis</td>
<td>Thomson Reuters</td>
<td>Government and Regulatory</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Julia Walker</td>
<td>Thomson Reuters</td>
<td>Head of Market Development, Risk &amp; Regtech, Asia</td>
<td></td>
</tr>
<tr>
<td>Bob Trojan</td>
<td>Token Insights</td>
<td>President and CEO</td>
<td></td>
</tr>
<tr>
<td>Gene Vayngrib</td>
<td>Tradle</td>
<td>CEO and Co-Founder</td>
<td></td>
</tr>
<tr>
<td>Celina Leung</td>
<td>TransUnion</td>
<td>Vice President and General Counsel, Asia-Pacific</td>
<td></td>
</tr>
<tr>
<td>Jiandi Zhang</td>
<td>Tsinghua University</td>
<td>Deputy Director, Institute for Fintech Research</td>
<td></td>
</tr>
<tr>
<td>Douglas Amor</td>
<td>University of Hong Kong</td>
<td>Kerry Holdings Professor in Law</td>
<td></td>
</tr>
<tr>
<td>Richard Lowe</td>
<td>UOB</td>
<td>Group Chief Data Officer</td>
<td></td>
</tr>
<tr>
<td>Vincent Voci</td>
<td>US Chamber of Commerce</td>
<td>Cyber Policy Director, Cyber, Intelligence and Security Division</td>
<td></td>
</tr>
<tr>
<td>James M. Sullivan, Jr.</td>
<td>US Department of Commerce</td>
<td>Deputy Assistant Secretary for Services</td>
<td></td>
</tr>
<tr>
<td>Matthew Mohlenkamp</td>
<td>US Department of the Treasury</td>
<td>Financial Attaché for Southeast Asia</td>
<td></td>
</tr>
<tr>
<td>Carol Cohen</td>
<td>US Department of the Treasury</td>
<td>International Economist</td>
<td></td>
</tr>
<tr>
<td>Kay Turner</td>
<td>US Department of the Treasury</td>
<td>Economist</td>
<td></td>
</tr>
<tr>
<td>Amy Zuckerman</td>
<td>US Department of the Treasury</td>
<td>Presidential Management Fellow</td>
<td></td>
</tr>
<tr>
<td>Emilio W. Cividanes</td>
<td>Venable LLP</td>
<td>Partner</td>
<td></td>
</tr>
<tr>
<td>Stuart Ingis</td>
<td>Venable LLP</td>
<td>Chairman</td>
<td></td>
</tr>
<tr>
<td>Margaret Miller</td>
<td>World Bank</td>
<td>Lead Financial Sector Economist, Finance, Competitiveness and Innovation</td>
<td></td>
</tr>
<tr>
<td>Fredesvinda Montes</td>
<td>World Bank</td>
<td>Senior Financial Specialist</td>
<td></td>
</tr>
</tbody>
</table>