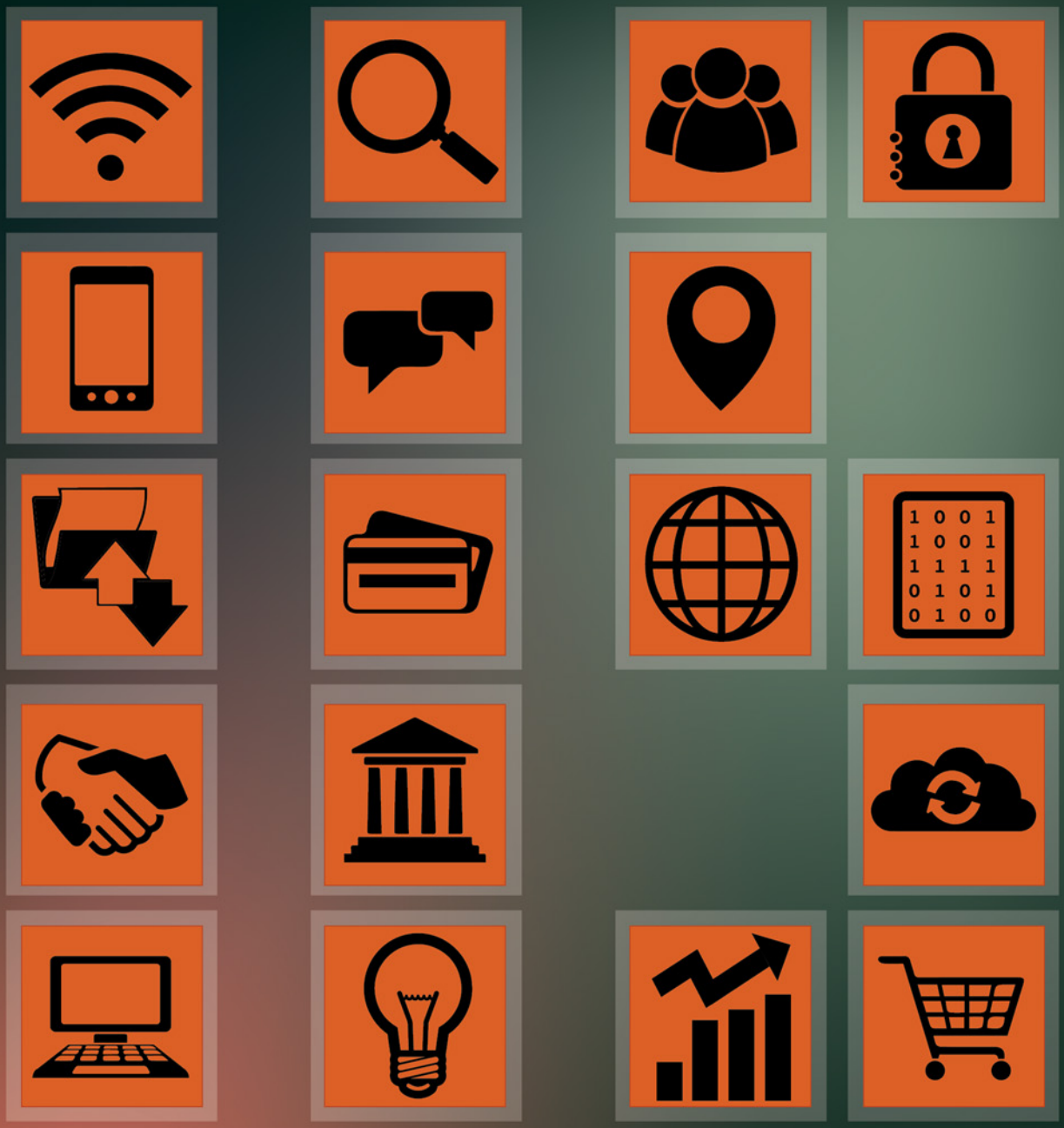

# Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System

**Report for APEC** **February 2016**

# Table of Contents

# 1. APEC and Privacy

APEC's primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region. Within this context, APEC plays an important role in the Asia-Pacific region in promoting a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of that information. The first significant component of this effort was the APEC Privacy Framework and the second was the Cross-border Privacy Enforcement Arrangement (CPEA). One of the most recent components of the framework is known as the APEC Cross Border Privacy Rules System (CBPR System).[1]

At February 2016, the CBPR System is just over 3 years old. It went public in July 2012 with the USA as the first economy to sign up. Four economies – the USA, Mexico, Japan and Canada – have adopted this voluntary system.[2] One accountability agent, TRUSTe in the USA, is currently certifying businesses against the CBPR System while another, JIPDEC in Japan, had just been approved at the time of writing. TRUSTe has approved in part or in whole fourteen businesses under the CBPR System to date.[3]

There is significant potential for the CBPR System to grow. More importantly, it could have a substantial impact on the further economic growth of the APEC region. Currently, APEC member economies account for approximately three billion people, half of global trade, 60 per cent of total GDP and much of the world's growth.[4] As such, upward or downward trade trends in this region have significant global impact. Trade is increasingly dependent on data and the transfer of personal information. The presence or absence of an effective system for safeguarding personal information will have a corresponding positive or negative impact on trade.

## 1.1 Objective

The APEC Secretariat engaged Annelies Moens and Malcolm Crompton from Information Integrity Solutions Pty Ltd (IIS) to undertake a preliminary assessment of possible benefits to economies and businesses joining the CBPR System from business, government and regulator perspectives. There is a strong need to assess and communicate the benefits of the APEC CBPR System at this early stage of development. Awareness and understanding of the CBPR System is low, which is in and of itself a limiting factor to the adoption of the CBPR System more broadly. The nature of the publicly available documentation, including on the APEC website (www.apec.org) and at the CBPR dedicated website (www.cbprs.org), is both incomplete and not always up to date. This contributes to the lack of awareness.

The assessment as outlined in this report is based on consultations with a sample of economies and stakeholders operating in business, government and regulatory environments. It is expected that APEC member economies and businesses will use this preliminary assessment to start the process of conducting a full cost/benefit analysis from their own economy perspectives.

### 1.1.1 Scope of report

This report is not intended to be exhaustive or conclusive, but rather serve as a catalyst to assist business, government and regulators to further assess the significance of the CBPR System. In

particular, the report intends to highlight the potential role of protecting the personal information of citizens and consumers in a way that increases trust and facilitates (rather than impedes) trade between economies. The report specifically focuses on the benefits of the CBPR System; it is not an assessment of pros and cons. The views provided in this report are generally provided by those consulted, as understood and expressed by the authors. As such, any errors in expressing the benefits are solely of the authors.

The scope of this project did not include any direct discussion with consumers or consumer stakeholder groups regarding their views of the CBPR System. This is largely due to the infancy of the CBPR System and the lack of awareness and understanding of the System. Anecdotally, a Singaporean-based stakeholder, who the authors consulted, conducted a review of Singaporean media publications and found that the CBPR System has only been mentioned once (in 2013 in an Asia Cloud Computing publication).

It should also be noted that this report does not address the recently released Privacy Recognition for Processors (PRP),[5] which is a subset of the CBPR System, as this was not within scope.

#### 1.1.1.1 Methodology

The consultations and drafting of this report occurred between December 2015 and February 2016. In that timeframe the authors were only able to select a sample of businesses (both participants and non-participants of the CBPR System), regulators and government representatives of APEC economies with whom to discuss their views of the CBPR System. The selected economies were those that have signed up to the CBPR System – USA, Mexico, Japan and Canada – as well as Singapore because it is an important trade hub.

Consultations with Japanese and Singaporean stakeholders took place in person and with stakeholders in the USA, Mexico and Canada by phone. Those that were able to provide their time and expertise to speak with the authors of this report about the benefits of the CBPR System are listed in Appendix 2. The authors have chosen not to quote stakeholders directly, as many did not want to be attributed and the authors did not want to impede the candid nature of the conversations and comments during consultations.

### 1.1.2 Context

The extent to which a given economy or stakeholder finds value in the CBPR System largely depends on the economy's underlying domestic law, the underlying domestic law of its current or future trading partners, and the requirements of stakeholders. As such, many of the benefits discussed in this report are important to consider in the context of the laws (or lack thereof) pertaining to cross-border data flows in the economy in question. Appendix 1 includes a summary of the legal position of cross-border data flows in the economies included in the reporting sample as understood by the authors. Please note, however, that this report – including the economy overviews – must not be construed as legal advice nor relied upon as such.

Generally, economies' laws on cross-border data flows fall into the following three categories:

1. No limitation on data export

2. No limitation on data export, but exporting party remains accountable
3. Data export not permitted unless certain exceptions are met

Additionally, some economies have environments where stakeholders are already accustomed to using certifications, such as the PrivacyMark for domestic data flows in Japan. Other economies are less accustomed to trustmark and certification processes.

Hence, while the legal regime governing cross-border data flows is a significant contextual aspect in determining the value of the CBPR System, it is arguable that what is more important is the current and future trading partners and their requirements, both from an import and export point of view. Thus trade requirements are likely to heavily influence the value of the CBPR System.

### 1.1.3 Summary of overall assessment

The awareness and understanding of the CBPR System is low, which is in and of itself a limiting factor to the adoption of the CBPR System more broadly. The extent to which economies and stakeholders find value in the CBPR System largely depends on each economy's underlying domestic law, the underlying domestic law of its current or future trading partners, and the requirements of stakeholders.

Businesses are key contributors to, and beneficiaries of, the CBPR System. They decide whether or not to join, while at the same time the value of the System increases with each additional participant. The third party validation and enforcement provides a level of assurance to external stakeholders. The independence and professionalism of accountability agents, privacy enforcement authorities and the Joint Oversight Panel (JOP, CBPR's oversight body) are integral to the credibility of the system and impacts the overall regulatory benefits (see Part 5 for the overall assessment).

# 2. Government Stakeholders

Governments representing APEC economies were largely responsible for the creation of the CBPR System for business. As such, the System has neutral application across different industries and it is therefore very different to industry-specific codes. In some economies, governments have signed up to the CBPR System with minimal or no consultation with business. In other economies, governments would not sign up to the CBPR System without the imprimatur of business.

Whether governments or businesses drive the adoption of the CBPR System, the following benefits are key considerations from a government stakeholder perspective.

## 2.1 Trade benefits

Trade benefits are decisive considerations in government's uptake of the CBPR System and the following sections outline some that have been highlighted in stakeholder consultations.

### 2.1.1 Advancement towards global trade and economic growth policy objectives

Most, if not all, economies have policies in some shape or form that are aimed at furthering economic growth and prosperity through trade. It has also been a strong and consistent theme in the activities of

APEC since its inception.[6] Going right back to the Bogor Goals, APEC economies recognise that global trade and economic growth cannot continue to trend upwards without a trusted environment for conducting trade. Personal information is an increasing cornerstone in trade, especially as service industries continue to grow and value is derived from the analysis and application of data.

Some economies have major interests in services that handle significant amounts of personal information from other economies, such as call centres. Mexico, for example, is an economy (like India, the Philippines and Uruguay) that provides a large range of data services which makes up a significant portion of its GDP. Likewise, Singapore is a major hub for data processing and analytics that handles financial information, human resources and employee data, among others.

Having data transfer arrangements and protections in place is important. As an example, from a Mexican perspective, Argentina gaining EU adequacy has meant that its data service industry has grown hugely due to business with Europe – so much so that a couple of stakeholders have described it as being as big as its wine industry.

The CBPR System contributes to supporting the advancement of global trade and economic growth by providing a scalable baseline set of privacy standards. As economies adopt localisation measures to protect domestic interests, the CBPR System becomes even more important to provide a gateway to alleviate those pressures in conjunction with arrangements such as the Trans Pacific Partnership (TPP). In particular, Article 14.8 (Personal Information Protection) in Chapter 14 of the TPP on Electronic Commerce provides that “each Party should encourage the development of mechanisms to promote compatibility between these different [legal] regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks”.[7]

### 2.1.2 International cooperation

The importance of international cooperation for diplomatic and other reasons also cannot be underestimated. The CBPR System, as an international data protection tool (albeit for the APEC region), has the potential to make connections with other international data protection frameworks, including in the EU. This has been recognised in the work on connecting the APEC CBPR System and EU Binding Corporate Rules (BCR) System through a common referential.[8]

The CBPR System potentially enables all 21 APEC economies to trade with one another using a common baseline privacy standard on a voluntary basis. Its reach is significantly wider than multilateral or bilateral agreements. While not a global data transfer regime, it makes significant inroads in covering a substantial part of the global economy, indeed the most populous and fastest growing economic region in the world.[9]

The CBPR System is designed to connect into domestic legal frameworks where there is an enforcement authority that can enforce the CBPR System. The System provides equal opportunity for all economies by:

- Not imposing the baseline APEC Privacy Framework standards on businesses operating in economies with lower or no requirements, unless and until the business voluntarily adopts them for trade or other reasons

- Co-existing with, rather than watering down, higher domestic data protection requirements where they exist.

### 2.1.3 Increased confidence

Anecdotally governments appear more concerned with the outsourcing of their citizen's data to other economies than commercial entities. This is increasingly so as awareness increases of both data breaches and misuses of personal information. The CBPR System could provide greater comfort and accountability with regards to the protection of data offshore. This becomes increasingly important with the continued advances in technologies such as big data analytics and automated algorithmic decision making.

### 2.1.4 Procurement processes

From a policy perspective, some governments have used procurement processes to implement government objectives when selecting suppliers to complete government contract work. This is evidenced in many different areas such as diversity requirements of suppliers, suppliers' adherence to ISO standards and so forth. In the trustmark space this has been seen in the Japanese context with certain Ministries requiring successful tenderers to have in place a PrivacyMark (the domestic privacy certification in Japan).

As such, from a policy point of view there is potential for participating economies in the CBPR System to require suppliers of government contracts to have CBPR certification in place. This would make suppliers with a CBPR certification more attractive to government. Businesses could also require other businesses to have CBPR certification in place prior to conducting business.

## 2.2 External stakeholder benefits

Governments generally seek to consider impacts on a broad spectrum of stakeholders when adopting policies, as not doing so tends to introduce unintended consequences. The following benefits consider the CBPR System from an external-to-government perspective, where the benefit to government is indirect.

### 2.2.1 Tool to maintain free flow of data with privacy protection

Data protection laws are accelerating globally, but particularly in the APEC region. In the last five years alone several economies in the APEC region have adopted or significantly modified data protection laws including: Singapore, Malaysia, Chinese Taipei, the Philippines, Peru, Hong Kong, Australia, Republic of Korea and Japan. Some APEC data protection laws specifically regulate cross-border data transfers, with varying degrees of strictness. With this increased regulation comes the need to create mechanisms to safely allow cross-border data flows while according appropriate protection to that data.

In responding to the risk of cross-border data flows, the alternative to safeguarding the data as it travels across borders is to restrict or stop data flows altogether. This is an option that is present in some APEC economies. For example, Russia's Federal Law 'On Personal Data' Nr 152-ФЗ dated 27 July 2006 was recently supplemented by a new requirement effective September 2015 which makes it

illegal to collect personal data of Russian citizens and send it directly to servers located outside Russia without involving a database installed on a Russia-based server/computer in the processing of the personal data.

The CBPR System is a tool that enables businesses to demonstrate compliance with a commonly understood set of privacy rules that apply across APEC and provides a level of certainty and predictability for business and privacy practices. In the absence of an effort like this, it will be more difficult to convince governments to move away from data localisation and other restrictions on the free flow of data.

### 2.2.2 Maintain trust in APEC economies

As noted earlier, we operate in a globally connected world, in particular the APEC region is a diverse region with approximately 40% of the world's population and half of the world's trade. It would be reasonable to assume that to a greater or lesser extent, data on citizens in each of these economies are processed, used, controlled in other APEC or global economies in addition to their own. Using frameworks that help maintain and build trust in the APEC region helps governments ensure that businesses are meeting and protecting the privacy of their citizens when the data are in other economies.

### 2.2.3 Assurance

The CBPR System provides for an external validation of businesses' privacy practices as well as an annual review process. Those additional checks and balances placed upon business and paid for by business provide a level of assurance to external stakeholders, including governments, that is generally above and beyond legal requirements.

# 3. Business Stakeholders

Businesses are key contributors to, and beneficiaries of, the CBPR System. On the one hand, the System exhibits a network effect in which the greater the number of participants, the greater the value and appeal of joining the System in order to take advantage of low-friction and protected transfers to other participants. On the other hand, participation in the System is voluntary, and so any step that appears at first blush to incur a cost to business without providing clear benefits will face an uphill battle to gain acceptance.

Consequently, our consultations with business stakeholders have been an important part of trying to elucidate those benefits at such an early stage of the System's operation. These benefits have been divided below into three categories: (i) trade benefits, (ii) benefits internal to the organisation and (iii) external stakeholder benefits which primarily relate to the impact on consumers as provided through the lens of business stakeholders.

## 3.1 Trade benefits

### 3.1.1 Appropriate privacy protection

Finding the right balance that promotes trade and protects privacy is critical. Both excessive privacy protection measures and inadequate privacy protection measures can have a negative impact on trade. For example, complex and varied data privacy regimes could force businesses with operations in different jurisdictions to dedicate considerable resources to compliance, which often devolves into an unproductive administrative exercise with minimal impact on individual privacy. The complexity and cost only increases as partners and contractors are inevitably added to the picture. For example, in today's globally connected economy, one can easily imagine the following scenario:[10]

- Company based in Country A
- With operations in Country B
- Capturing data on citizens in Countries A, B, C, and D
- Leverages a cloud service provider based in Country E
- Cloud service provider replicates data across facilities in Countries B, E, F, and G.

On the other hand, insufficient privacy protection measures also impede trade as can be seen recently by the reaction of German consumers to US cloud service providers in the wake of the Snowden revelations, where "opening a local office is virtually a requirement due to consumer concerns about cross-border data transfers and security outside of German borders".[11]

There is economic value to consumers and hence business benefit in being a good data steward. Reflecting the enormous contribution that the APEC region makes to global trade, in time the impacts on those businesses that are good data stewards and their customers could be enormous.

#### 3.1.1.1 Importing and exporting

The CBPR System increases privacy protection offered by participating businesses in economies where there is no data protection law, while not detracting from privacy protection in economies where there is data protection law that businesses must comply with.

For instance, businesses exporting data and individuals using their services could have more confidence exporting to economies without data protection law if businesses in those economies are CBPR participants. Likewise, businesses importing data from economies with data protection laws in place are more likely to be attractive data recipients with CBPR in place.

Export

As an example, in the Japanese context there is greater concern over data exports than imports. Japanese businesses send lots of data to China, in particular, to the Dalian area which provides significant call centre services for Japanese businesses. The transfer of this data to China has been largely unregulated and any governance is provided through contracts. Japanese businesses exporting data could more easily be assured that management of the data in China meets expectations of their customers if the Chinese entities were CBPR-certified.

Vietnam and Thailand also provide outsourcing services to Japanese companies. Here too, Japanese businesses need to manage the risks of data export either by contract or, potentially more simply, by outsourcing to CBPR-certified businesses located there.

Likewise, stakeholders consulted in Singapore indicated CBPR could be very useful to service providers who deal with clients on a business-to-business basis that may have preferences around where data is located. CBPR certification could help overcome domestic prejudice, especially where business clients are worried about varying standards in different economies. If CBPR were in place at least it could be said that a baseline standard was being used, regardless of where data was being sent for processing. The effective rule of law, however, was still an important consideration in choosing location of data processing.

Import

For economies receiving or wanting to receive data from economies with good privacy protection, CBPR has the potential to provide a baseline level of assurance to the exporting economy. The logic is simply the inverse of the export examples given earlier.

As mentioned, China, Vietnam and Thailand among others provide outsourcing services to Japanese companies. Economies that have minimal or no data protection laws in place could arguably make themselves more attractive as data importing economies if those economies joined the CBPR System and businesses there were CBPR-certified.

For example, China submitted a case study of China Tea Net to the Data Privacy sub-group meeting in Moscow in 2012 which states in section IV, 'CBPRs: Facilitating and International Market Presence', that if China Tea Net "makes use of policies and procedures in place that are consistent with the globally-accepted standards such as those embodied in the APEC Privacy Framework it can provide China Tea Net the opportunity to further promote such trust".[12]

#### 3.1.1.2 Small and medium enterprise

Some data protection laws in the APEC region including Singapore and Japan apply to small and medium enterprises, not just to big business. Small and medium enterprises comprise the vast majority of businesses. For example, in ASEAN economies which are also APEC economies (except for Cambodia, Laos and Myanmar), over 96% of businesses are small and medium enterprises.[13]

Small and medium enterprises generally don't have their own legal counsel or resources to roll out expansive privacy programs. Small and medium enterprises whose core business revolves around data import or export could benefit from applying the CBPR System as a baseline standard.

### 3.1.2 Interoperability

How regional frameworks can connect to other regional frameworks is important from a global perspective, which is a perspective that is increasingly important for businesses and governments to consider. The CBPR System, as an APEC regional framework, has the potential to make connections with other international data protection frameworks, such as EU BCR.

Work on connecting the APEC CBPR System and BCR System in the EU through a common referential is significantly underway. One CBPR-certified company that the authors consulted has already used the referential to obtain BCR certification quicker and cheaper on the basis of its CBPR certification (see Part 3.2.2 below).

### 3.1.3 Foreign direct investment

CBPR may positively impact foreign direct investment. Japanese stakeholders were of the view that Japan would invest more in economies where there is no data protection law in place if those economies and businesses participated in the CBPR System.

Japan, as do many other APEC economies, invests heavily in developing APEC economies. An example provided was Japan's IT investment in Vietnam and Myanmar's customs clearance procedures, to facilitate the increased trade in goods which need to be processed and cleared by customs officials in those economies. Japan's IT technology enables procedures for import and export to be carried out by inputting and transmitting the necessary data just once.[14]

These improved facilities for Vietnam and Myanmar positively impact the rest of the APEC region as frictions on trade are reduced. CBPR may be another tool to assist with decreasing friction in trade.

## 3.2 Internal organisational benefits

### 3.2.1 Future proofing for change

Businesses wanting to expand globally and hence transfer data across jurisdictions need to consider the way they will structure their data handling policies to make it as easy as possible to enter new markets and adapt to the changing regulatory landscape.

This is particularly important as more and more economies regulate cross-border data transfers due to concerns with how this is managed. Adopting regional baseline standards such as the CBPR System has the potential to make the transition smoother when entering new markets and complying with increased privacy obligations.

### 3.2.2 One global compliance system

The APEC region is diverse, with many different cultures. Having a common set of baseline standards which are interpreted in the same way can help overcome cultural differences that would otherwise make cross-border data transfers even more complex.

Businesses that are operating globally could benefit from a simplified compliance system if they could adopt one standard across all their operations with the potential benefit to end user privacy that resources are focused on better privacy rather than complex layers of compliance. Regional frameworks that can be integrated with other such frameworks make this process easier.

One CBPR-certified company that the authors consulted has benefited greatly from its CBPR certification because it lowered the cost and time involved in obtaining its BCR certification in the EU for its existing global privacy program. Had it approached the BCR process without having done the CBPR certification first, this would have slowed the process significantly.

In that example, the first phase of the company's BCR review took 2.5 months and the mutual recognition phase 9 months, with a slight delay due to issues with the Safe Harbor Framework that were outside of its control. According to the company, the whole process was four months shorter than the average time taken for a BCR approval of 18 months.

Having based its BCR certification on the CBPR framework and the common referential, not much was required to be changed internally within the business and thus significant expense was spared. Its overall cost of obtaining BCR as a result of obtaining CBPR certification first was approximately 90% less than had it not obtained CBPR certification.

### 3.2.3 Efficiency

Some stakeholders considered that the CBPR System would provide for efficiency in business negotiation where the focus between CBPR-certified businesses could be on the actual business transaction rather than the regulatory burden, as a common standard could be relied upon as a good starting point.

Likewise, new products and services could be rolled out to market more quickly as the internal regulatory review processes could be conducted faster.

### 3.2.4 Flexibility

The CBPR System could be considered a more flexible model than existing cross-border data transfer mechanisms such as contracts or model clauses. An emerging challenge is the myriad of contracts that might be required with all other parties in a supply chain, some of which may need to change or be added to at short notice and cover only limited periods. For example, depending on how clauses are drafted within contracts, if a supplier changed, then everything would have to be redone. Under the CBPR System, it would be possible to simply move to a new supplier, if required, in real-time.

The CBPR System is sufficiently flexible that it allows businesses to have flexibility as to the data to which it applies and the economies that will be covered – this is outlined in the application forms that businesses must submit for their certification. The scope of existing certifications can be found in the APEC CBPR Compliance Directory.[15]

For example, one CBPR-certified company chooses to apply the CBPR System to a narrow data set. According to its global privacy policy, the certification only covers information that is collected through its website and does not cover information that may be collected through downloadable software, SaaS offerings, or mobile applications.

Another CBPR-certified company limits the economies to which CBPR applies. Its global privacy policy indicates that CBPR applies to its business processes across its operations that transfer personal information from its affiliates in the U.S. to its affiliates in other APEC member economies. It anticipates that its affiliates in other APEC member economies will obtain certification for transfers of personal information that originate in those economies after those economies are approved as participants in the APEC CBPR system.

### 3.2.5 Regulatory treatment

Businesses that adopt the CBPR System are, in some instances, voluntarily agreeing to be regulated by a privacy enforcement authority where otherwise they would not be regulated. For example, this would be the case for businesses in economies that do not have data protection legislation in place, or businesses that would otherwise be exempt from data protection legislation (such as a small business in a jurisdiction's whose data protection legislation does not regulate small businesses).

Businesses in such situations would consider whether or not they wish to have the extra potential regulatory oversight, which can be influenced by the robustness of privacy programs in place. Some businesses were of the view that frameworks such as the CBPR System allow businesses to develop a greater tolerance for risk, because they feel more confident in their management of data and thus are more able to tolerate risk. On the other hand, some businesses thought the CBPR System would not change their risk appetite.

Nevertheless, regardless of whether or not businesses would ordinarily be regulated by a privacy enforcement authority, how an authority would treat them is of significant interest to those contemplating or obtaining CBPR certification.

A number of the business stakeholders consulted were of the view that regimes where accountable third parties are involved in certification practices provide businesses more credibility with regulators. Privacy enforcement authorities may look favourably on businesses that are CBPR-certified, though this does not inoculate against enforcement action. Privacy enforcement authorities are generally not in a position to promise favourable treatment as they must remain independent and not compromise their ability to enforce requirements. However, in the authors' experience as ex-regulatory staff, the reality is that most regulators would in practice consider steps taken by business to safeguard privacy in determining what enforcement actions and/or remedies are required.

## 3.3 External stakeholder benefits

Stakeholders consulted were confident that there would be a range of general benefits to external stakeholders such as consumers, although at this stage there is little hard evidence. Some of these potential benefits are set out here.

### 3.3.1 Assurance

The CBPR System is based on an external validation model with:

- Accountability agents (which can be public or private sector entities) that determine whether requirements for the certification have been met, and
- A privacy enforcement authority that can enforce the requirements of the System.

It is not dissimilar to financial regulatory systems, in that auditors sign off on accounts and financial regulators have oversight and can take enforcement action where needed. There is also an annual review process in the CBPR System – much like in the financial system – where financial accounts are reviewed annually. The main difference in the CBPR System is that the 'auditors' (the

accountability agents) also handle consumer complaints about the businesses they certify as being compliant with the CBPR System.

The third party validation and enforcement provides a level of assurance to external stakeholders. The independence and professionalism of accountability agents, privacy enforcement authorities and the Joint Oversight Panel (which oversees accountability agents and processes the applications of economies) are integral to the credibility of the system.

### 3.3.2 Communication with consumers

Communicating privacy information to consumers can be complex. This is evidenced by the lengthy privacy policies and notices that businesses produce which often give the consumer the impression that they should not be read and that they give permission to the business to do whatever they like with their personal information.

Having standards in place makes it easier to communicate with consumers – saying that you comply with an international data protection standard is simple. Creating awareness of that standard, however, requires more effort.

### 3.3.3 Trust

The fundamental aim of the CBPR System is to increase the level of trust that external stakeholders, in particular consumers, can place in certified businesses. At this early stage in the operation of the CBPR System it is too early to say whether it actually increases trust. For trust to increase consumers need to recognise the certification in the first place, see it in place across a wide number of businesses and economies and experience the benefits such as better complaint handling and better management of their personal information.

Business-to-business trust levels could also potentially be increased when businesses engage with CBPR-certified businesses, presuming again that those businesses understand what the certification means and value it.

### 3.3.4 Good faith and public relations

CBPR certification could assist businesses to demonstrate stewardship of personal information and help show good faith when faced with regulatory action. Businesses may also use the certification to help promote products and services that involve cross-border data transfers.

# 4. Regulator Stakeholders

The backbone of the CBPR System is the Cross-border Privacy Enforcement Arrangement (CPEA). The CPEA enables privacy enforcement authorities to work together to resolve matters including where regional cooperation for enforcement may be required.

The CBPR System enables consumers to lodge complaints with the accountability agent and/or privacy enforcement authority. Generally, most consumers complain to the relevant business first,

then to the accountability agent. If they are dissatisfied with the resolution they can complain to the privacy enforcement authority.

The addition of accountability agents to the dispute resolution framework is an integral part of the CBPR System and is key to the effectiveness of the regime.

## 4.1 Internal regulatory benefits

The CBPR System has the potential to broaden the set of actors that play a role beyond the privacy enforcement authority. The introduction of accountability agents as both 'auditors' and 'dispute resolvers' has the potential to increase significantly the resources available for ensuring businesses are accountable for their privacy practices and also impact on the role of privacy enforcement authorities and where they place their attention and resources.

It should be noted, however, that current accountability agents do not cover businesses operating in all sectors of the economy. For example, in the USA, the Federal Trade Commission is currently the only relevant privacy enforcement authority. It does not have jurisdiction over sectors including health, not-for-profit organisations and aspects of the financial services industry. Accordingly, business operations in these sectors cannot as yet be part of the CBPR System and TRUSTe cannot be an accountability agent for these sectors.

Similarly, JIPDEC – the newly approved accountability agent for CBPR in Japan – was established by the Ministry of Economy, Trade and Industry of Japan (METI). As such its sectoral remit is limited to that covered by METI, which notably excludes the telecommunications and health sectors. So, in Japan pending implementation of the amended data protection law, the accountability agent can only cover the sectors within its remit as covered by METI. Once the amendments come into effect, and the privacy enforcement authority obtains jurisdiction over all sectors, then the accountability agent, likewise, will have the ability to certify businesses in all sectors.

### 4.1.1 Role of accountability agents and their overseers

The effectiveness of both accountability agents and their overseers (the Joint Oversight Panel) is crucial to the success of the CBPR System. Inadequate accountability agents or poor oversight would negatively impact the System. The CBPR System is designed to have checks and balances in place for accountability agents when first joining the System, as well as annual reviews to ensure continued trust and effective operation.[16]

In Japan, JIPDEC handles complaints from individuals and has been providing businesses with the domestic 'PrivacyMark' for more than 20-25 years. In that time only one company has had its PrivacyMark withdrawn – Benesse Holdings Inc, which is Japan's largest provider of distance education for children. The company's PrivacyMark was withdrawn in 2014 after it suffered a data breach that compromised the personal information of millions of its customers.[17]

In the USA, TRUSTe (the CBPR accountability agent for businesses headquartered in the USA) was the subject of a FTC investigation for failing to recertify companies under the now-defunct Safe Harbor Framework. The company agreed in 2014 to a consent order under which it must provide the FTC with an annual sworn statement with information about its certification programs, for a period of ten years.[18]

On the whole though, stakeholders express a significant level of trust in accountability agents. For example, JIPDEC is considered to be a very credible and trustworthy organisation, while the Joint Oversight Panel has passed TRUSTe's annual renewal requirements.

Maintaining high expectations of accountability agents needs to be balanced by the costs businesses are willing to pay for certification. The nature of accountability agents in terms of whether they are commercial, not-for-profit or public can have a bearing on expected market and regulatory outcomes. The independence and professionalism of accountability agents, privacy enforcement authorities and the Joint Oversight Panel are important and impacts the overall regulatory benefits, as outlined below.

### 4.1.2 Improved strategic resource allocation

The CBPR System has the potential to allow privacy enforcement authorities to focus their efforts and resources on systemic, high profile and high impact privacy issues, rather than first line complaint handling which accountability agents can handle in the first instance. With successful complaint handling, an accountability agent can positively impact the workload of privacy enforcement authorities to enable them to focus their efforts strategically.

For example, in the Japanese context in relation to its domestic PrivacyMark, JIPDEC managed 125 complaints for the period April 2014 to March 2015 and METI (which is also the relevant privacy enforcement authority in the CBPR System for that sector in Japan) managed 194 complaints. According to direct sources the authors spoke with, in the US context, TRUSTe managed 75 complaints under the CBPR System for the period 1 June 2014 to November 2015. Of those, 5% led to certified companies changing their privacy practices. The authors were advised that the FTC has not received any CBPR complaints.

## 4.2 External regulatory benefits

A number of external regulatory benefits, which are indirect benefits to regulators, have also been identified as outlined below.

### 4.2.1 Assurance

The CBPR System is still in its infancy in terms of its application. However, it is designed and structured in such a way as to provide external validation to regulators as well as other stakeholders. The role of third parties in assessing compliance against a standard is a well understood concept globally in many sectors, such as the finance, IT and medical sectors, to name a few.

Accountability agents are also subject to annual reviews. The CPEA that supports the CBPR System also enables redress locally and globally.

The CBPR System provides a way for businesses to demonstrate their privacy practices to accountability agents and regulators. When enforcement action happens, arguably the System makes it easier to demonstrate the privacy practices that are in place.

### 4.2.2 Choice

Adding the avenue for redress through accountability agents provides consumers with another option for handling their complaint. While consumers may still go directly to privacy enforcement authorities to handle their complaint, it is common to find in regulatory handling processes a requirement that other avenues initially handle complaints. Privacy enforcement authorities can then hear appeals where required.

### 4.2.3 Raises the benchmark

For businesses operating in economies that do not have data protection law in place, or have levels of protection that are lower than the CBPR System, CBPR raises the benchmark for those businesses who adopt CBPR in terms of the standards which they seek to meet. Raising the benchmark may also help to level the playing field for those businesses that already engage in good privacy practices.

The baseline standard provided by the CBPR System also helps businesses to manage risk better in situations where it is not always possible to seek consent from customers, or it is unclear as to where data will be transferred.

In economies where data protection laws are in place or standards higher than the CBPR System are in place, these obligations would still need to be followed as CBPR does not replace domestic laws.

# 5. Overall Assessment

The awareness and understanding of the CBPR System is low, which is in and of itself a limiting factor to the adoption of the CBPR System more broadly. The consultations show this challenge starts with the nature of the documentation available to interested parties on the APEC website, the CBPR System website and elsewhere, as well as the minimal publicity and outreach that have occurred with the limited resources that have been made available.

APEC economies conduct approximately half of the world's trade. As such, trends upward or downward in this region have significant global impact. Global trade and economic growth cannot continue to trend upwards without a trusted environment for trade. Trade is increasingly dependent on data and transfer of personal information, especially as service industries continue to grow and value is derived from the analysis and application of data.

The extent to which economies and stakeholders find value in the CBPR System largely depends on economies' underlying domestic law, the underlying domestic law of their current or future trading partners, and the requirements of stakeholders. Trade benefits are decisive considerations in the uptake of the CBPR System. The CBPR System contributes to supporting the advancement towards global trade and economic growth policy objectives by providing a scalable baseline set of privacy standards. It also has the potential to make connections with other international data protection frameworks, such as the EU BCR framework.

Data protection law is accelerating globally, but particularly in the APEC region. Finding the right balance that promotes trade and protects privacy is critical. Excessive privacy protection measures and inadequate privacy protection measures both negatively impact trade. Businesses are key

contributors to, and beneficiaries of, the CBPR System. They decide whether to join or not, while at the same time the value of the System increases with each additional participant. Businesses exporting data could have more confidence exporting to economies without data protection law if those economies and businesses had CBPR in place. Likewise, businesses importing data from economies with data protection laws are more likely to be attractive data recipients with CBPR in place.

Adopting regional baseline standards such as the CBPR System has the potential to make the transition smoother when entering new markets and complying with increased privacy obligations. Having a common set of baseline standards which are interpreted in the same way can help overcome cultural differences that would otherwise make cross-border data transfers even more complex.

The role of third parties in assessing compliance against a standard is a well understood concept globally in many sectors, such as the finance, IT and medical sectors, to name a few. The third party validation and enforcement provides a level of assurance to external stakeholders. The independence and professionalism of accountability agents, privacy enforcement authorities and the Joint Oversight Panel are integral to the credibility of the system and impacts the overall regulatory benefits.

It is expected that APEC member economies and businesses will use this preliminary assessment to start the process of conducting a full cost/benefit analysis from their own economy perspectives.

# 6. References


[1] See APEC, *APEC Cross-Border Privacy Rules System* <http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf>.

[2] The four acceptance reports can be found here:

- US, <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/BBDCED12534F4EA48F3542D03AFD56B9.ashx>
- Mexico, <http://inicio.ifai.org.mx/English/7%20Mexico's%20Findings%20Report_APEC%20CBPR.pdf>
- Canada, <http://www.apec.org/~/media/Files/Groups/EC/APEC%20Canada%20Joint%20Oversight%20Panel%20Findings%20Report%20April%202015.pdf>
- Japan, <http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/20140430_CBPR_Japan_Final_Report.pdf>.

[3] TRUSTe, 'TRUSTe Certified Companies' <https://www.truste.com/consumer-resources/trusted-directory/>.

[4] APEC, '2015 APEC economic leaders' week opens in Manila' (13 November 2015) <http://www.apec.org/Press/News-Releases/2015/1113_CSOM.aspx>.

[5] APEC, *Privacy Recognition for Processors: Purpose and Background* (February 2015) <https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf>.

[6] APEC, 'About APEC: History' <http://www.apec.org/About-Us/About-APEC/History.aspx>.

[7] Trans-Pacific Partnership Agreement, 'Chapter 14: Electronic Commerce' <http://dfat.gov.au/trade/agreements/tpp/official-documents/Documents/14-electronic-commerce.pdf>.

[8] Article 29 Working Party and APEC Economies, *Referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents* (March 2014) <http://www.apec.org/~/media/files/groups/ecsg/20140307_referential-bcr-cbpr-reqs.pdf>.

[9] See Matikas Santos, '#InquirerSeven fast facts you need to know about APEC members' (17 November 2015) <http://globalnation.inquirer.net/131270/inquirerseven-fast-facts-apec-members-economy-tourism-population-internet-philippines>.

[10] Asia Cloud Computing Association, *The Impact of Data Sovereignty on Cloud Computing in Asia Summary Report* (12 March 2014) <http://www.asiacloudcomputing.org/images/research/DataSovereigntyReport2013_ExecutiveSummary.v2.pdf>, p. 6; Information Integrity Solutions, *Success Through Stewardship: Best Practices in Cross-Border Data Flows* (23 January 2015)

<http://www.iispartners.com/downloads/IIS_Success_through_stewardship_Best_practice_in_cross_border_data_flows.pdf>, p. 20.

[11] International Trade Administration, *2015 Top Markets Report Cloud Computing: A Market Assessment Tool for US Exporters* (July 2015) <http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf>, p. 13.

[12] China, *APEC Cross Border Privacy Rules Case Study: China Tea Net (2012/SOM1/ECSG/DPS/007)* (1 February 2012) <http://mddb.apec.org/Documents/2012/ECSG/DSP1/12_ecsg_dps1_007.pdf>, p. 4.

[13] Ted Tan, 'Keynote speech at the ASEAN SME Working Group Meeting' (11 June 2014) <http://www.spring.gov.sg/NewsEvents/PS/Pages/Keynote-speech-by-Ted-Tan-at-the-ASEAN-SME-Working-Group-Meeting-20140611.aspx?skw=aec%202015>.

[14] Dang Cong San, 'Vietnam's modernized e-customers to begin in early April' (31 March 2014) <http://www.talkvietnam.com/2014/03/vietnams-modernized-e-customs-to-begin-in-early-april/>; JIFFA, 'Japan's NACCS to provide technical support to Myanmar customs' (15 June 2010) <http://www.jiffa.or.jp/en/news/entry-3562.html>.

[15] The directory is accessible from the CBPR System home page: <http://www.cbprs.org/>.

[16] APEC, 'Ongoing APEC CBPR requirements for Accountability Agents' <http://www.cbprs.org/Agents/OngoingRequirements.aspx>.

[17] Nikkei Asian Review, 'Customer data leak deals blow to Benesse' (10 July 2014) <http://asia.nikkei.com/Business/Companies/Customer-data-leak-deals-blow-to-Benesse>.

[18] Federal Trade Commission, 'TRUSTe settles FTC charges it deceived consumers through its privacy seal program' (17 November 2014) <https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.

# 7. Appendix 1 – Economy Overviews

## 7.1 Japan

Japan has had data protection law – the Act on the Protection of Personal Information (APPI) since 2003, which regulates the private sector. The Minister of Internal Affairs and Communications has oversight of the public sector under separate legislation in relation to data protection.

In September 2015, amendments were made to the APPI which for the first time introduce cross-border data provisions. The amendments will come into effect before September 2017.

Currently, the Minister in each industry sector enforces the APPI. On 1 January 2016, the new enforcement entity is the Personal Information Protection Commission (PPC), which operated between 1 January 2014 and 31 December 2015 as the 'Specific' Personal Information Protection Commission responsible for oversight of Japan's ID Number System. The enforcement by the PPC, which replaces the Ministers in each industry sector, will start after the main amendments come into force.

The new cross-border data provisions, located in Article 24, allow cross-border data transfers if consent of the individual is obtained to transfer to the specific recipient in an overseas country. Should consent not be sought or provided, then the transfer could still take place if one of the following two conditions are satisfied:

1. Transfer to offshore countries that the PPC determines have measures of protecting personal information equivalent to that of Japan
2. The third party maintains an internal personal information protection system consistent with standards set by the PPC.

The PPC Rules that accompany the APPI to assist with its implementation and interpretation are currently in draft mode. They indicate that condition two may include a contract or rules being in place with the offshore entity and may also potentially be satisfied through the CBPR System. In May 2014, Japan joined the CBPR System, the third economy to do so.

## 7.2 Singapore

Singapore's Personal Data Protection Act (PDP Act) was introduced in 2012 and came into effect on 2 July 2014. The Act introduced a framework for personal data protection in private sector organisations based on the concepts of consent, purpose and reasonableness. The Personal Data Protection Commission of Singapore administers and enforces the PDP Act.

The PDP Act has a specific provision dealing with the transfer of personal data outside Singapore (s 26). It provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDP Act.

Part III of the PDP Regulations 2014 specifies the requirements for transfers of personal data outside Singapore. The general regulation (s 9(1)) is that the transferring organisation must take appropriate steps to:

- Ensure that it will comply with the rules regarding protection of personal data while it remains under its possession or control, and
- Ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations to provide at least a comparable standard of protection to the Act. Examples of legally enforceable obligations include (s 10):
    - Law
    - Contract
    - Binding corporate rules, in the case of intra-group transfers
    - Any other legally binding instrument.

The organisation is deemed to have satisfied the requirement to take appropriate steps to ensure that the recipient is bound by legally enforceable obligations, in the following situations (s 9(3)):

- The data subject has given appropriate consent
- The transfer is necessary for the performance of a contract:
    - Between the organisation and the individual
    - Between the organisation and a third party entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest
- The transfer is necessary for a use or disclosure where consent is not required under the PDP Act, e.g., to respond to an emergency situation or it is in the national interest
- The personal data transits through Singapore to another location without being accessed, used or disclosed in Singapore
- The personal data is publicly available in Singapore.

## 7.3 USA

The United States does not have a general privacy law for private sector organisations. Instead, there is a series of sectoral and specialised privacy laws, both federally and among the states. The laws tend to address particular types of information, such as financial information, credit reports, health information, social security numbers and children's information online.

The Federal Trade Commission (FTC) has jurisdiction over the privacy practice of private sector organisations through the general consumer protection law that prohibits 'unfair or deceptive acts or practices in or affecting commerce' (FTC Act, s 5). The FTC can take enforcement action in this context against organisations that engage in:

- Unfair acts or practices – e.g., Company A transfers personal information that was provided for a particular purpose in a completely unrelated and unexpected way
- Deceptive acts or practices – e.g., Company B transfers personal information to a place that is not on the list of jurisdictions contained in its privacy policy; Company C communicates that overseas recipients adopt its own high security standards, but fails to ensure that they actually do so.

Once an organisation has been found to engage in unlawful behaviour, the FTC can require the organisation to take enforceable remedial steps, such as the implementation of comprehensive privacy and security programs, regular audits, and provision of notice and choice mechanisms.

There are no legal restrictions on cross-border data transfers. However, the FTC is the nominated cross-border privacy enforcement authority and thus has jurisdiction over businesses that are CBPR-certified in terms of their privacy practices affecting cross-border data flows.

## 7.4 Canada

In Canada, the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (PIPEDA) is the general privacy law for private sector organisations, subject to certain exceptions. PIPEDA contains a set of privacy principles that govern the collection, use, disclosure, accuracy and security of personal information, as well as the rights of individuals to know about, access and challenge the handling of their personal information. The Office of the Privacy Commissioner oversees the operation of the Act.

Relevantly for cross-border data flows, PIPEDA regulates the transfer of personal information across provincial and/or international borders for commercial activities. PIPEDA does not refer specifically to cross-border transfers. Rather, the Act broadly permits the transfer of personal information to a third party, subject to the accountability principle (Principle 1).

Principle 1 states that “an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party” (PIPEDA, Schedule 1, 4.1.3). In its Guidelines for processing personal data across borders (January 2009), the Office of the Privacy Commissioner clarified that “transfer” is a use, such that any personal information that is transferred can generally only be used for the purposes for which it was originally collected.

## 7.5 Mexico

Mexico's general privacy law, the Federal Law for the Protection of Personal Data in the Possession of Private Parties (PPD Law), came into effect on 6 July 2010. The Rules of the Federal Law for the Protection of Personal Data in the Protection of Private Parties (PPD Regulation) supplemented the PPD Law in December 2011. The Federal Institute for Access to Information and Data Protection of Mexico administers the PPD Law.

The PPD Law and Regulation specifically regulate the transfer of personal data to third parties (both domestic and foreign). The legal framework distinguishes between whether the recipient is a data processor or not. Nevertheless, in both cases the recipient is obliged to protect personal data in accordance with the PPD Law and Regulation, and any other applicable regulations.

Transfers involving data processors

Once a contractual relationship exists between a data controller and a data processor, cross-border transfers between them may occur without notifying the data subject or obtaining consent (PDP Regulation, Article 43). The contract must expressly establish a set of obligations for the data processor, including that it must adopt the necessary safety measures according to PPD Law and Regulation, and to only process or transfer personal data according to the instructions of the data controller. Under the PPD Regulation, communicating personal data to a data processor does not constitute a 'transfer' (Article 60).

If the data processor uses or transfers personal data in a way that violates the agreed terms, it will be deemed a data controller and take on the attendant obligations and responsibilities.

Transfers to third party recipients other than data processors

For recipients other than data processors, the PPD Law provides that cross-border transfers are permitted where (Articles 36 and 37):

- The data subject has consented through the privacy notice
    - There are several exceptions to obtaining consent – most notably, the data controller may transfer personal data without consent to a subsidiary, affiliate or any company within the same group as the data controller, provided that the recipient operates under the same internal processes and policies
- The data controller provides the recipient with the privacy notice and the purposes to which the data subject has limited the data processing, and
- The recipient assumes the same obligations as the data controller that has transferred the data.

These obligations include specific ones set out in the PPD Regulation, including adopting measures to guarantee due processing of personal data (Article 40) as well as security measures (Articles 49-59). The data controller must guarantee that the receiver will comply with these obligations through contractual clauses or other mechanisms.

# 8. Appendix 2 – Stakeholders Consulted

## 8.1 Government

**JAPAN**

| Name | Position | Organisation |
|---|---|---|
| Kiyomi Sakamoto | International Affairs Office, Commerce and Information Policy Bureau | Ministry of Economy, Trade and Industry |
| Rio Miyaguchi | Information Economy Division, Commerce and Information Policy Bureau | Ministry of Economy, Trade and Industry |
| Kazunori Yamamoto | Counsellor | National Strategy Office of Information and Communications Technology, Cabinet Secretariat |
| Emi Maeda | Senior Specialist, Attorney at Law, Office of Personal Information Protection, Legal System Planning Division | Consumer Affairs Agency |

**USA**

| Name | Position | Organisation |
|---|---|---|
| Michael Rose | Policy Advisor, Office of Digital Services Industries | Department of Commerce |
| Andrew Flavin | unknown | Department of Commerce |

**CANADA**

| Name | Position | Organisation |
|---|---|---|
| Daniele Chatelois | Manager, Privacy Policy, Electronic Commerce Branch | Industry Canada |

No government representatives were available from Singapore or Mexico.

## 8.2 Business

**JAPAN**

| Name | Position | Organisation |
|---|---|---|
| Jun Nakaya | Manager, Public Policy and Business Development Office | Fujitsu Limited |
| Yoshitaka Sugihara | Head of Public Policy and Government Relations | Google Japan Inc. |
| Toshiki Yano | Public Policy and Government Relations Counsel | Google Japan Inc. |
| Yukihiro Shirakawa | Director of Government & External Relations Planning Department | Hitachi Limited |
| Junichiro Asano | Manager, Government and Regulatory Affairs | IBM Japan Limited |
| Yusuke Koizumi | Senior Fellow, Information Society Research Department | Institute for International Socio-Economic Studies |
| Shintaro Nagaoka | Intellectual Property and Technology Department | Japan Electronics & Information Technology Industries Association |
| Junko Kawauchi | Vice President, Global Affairs | Japan Information Technology Services Industry Association |
| Soichi Tsukui | Manager, Executive Secretariat, Corporate Communications Division | KDDI Corporation |
| Toshinori Kajiura | Chair, Cyber Security Working Group | Keidanren (Japanese Business Federation) |
| Satoshi Tsuzukibashi | Director, Industrial Technology Bureau, Committee on Defense Industry Secretariat | Keidanren (Japanese Business Federation) |
| Tsukumo Mizushima | Department Manager, Customer Information Security Office | NEC Corporation |
| Shintaro Kobayashi | Senior Consultant, ICT & Media Industry Consulting Department | Nomura Research Institute |
| Keisuke Mizunoura | Senior Researcher, Social System Consulting Department | Nomura Research Institute |
| Makoto Yokozawa | Market and Organization Informatics Systems | Nomura Research Institute |

| Name | Position | Organisation |
|---|---|---|
| Tatsuya Yoshimura | External Relations Manager, External Relations & Trade Affairs Department | Sony Corporation |
| Motonori Yoshida | Specialist, Personal Data Protection Group | Toshiba Corporation |

**SINGAPORE**

| Name | Position | Organisation |
|---|---|---|
| May-Ann Lim | Director | Asia Cloud Computing Association |
| Boon Poh Mok | Director, Policy – APAC | BSA The Software Alliance |
| Lih Shiun Goh | Country Lead, Public Policy and Government Affairs | Google Singapore |
| Darryn Lim | Director, Trade & Innovation | Microsoft |
| Chan Yoon | Corporate Attorney, Legal & Corporate Affairs | Microsoft |
| Simon Smith | Director, Regulatory Affairs – Pacnet | Telstra |
| Peter Lovelock | Director | TRPC |
| Magnus Young | Senior Research Manager | TRPC |
| Additionally the authors met with the data protection officers and related roles at 15 companies in Singapore (4 of whom wish to remain unnamed), including: | | Apple<br>Accenture<br>DBS Bank<br>Deutsche Bank<br>General Electric<br>International SOS<br>Mastercard<br>OCBC<br>Standard Chartered<br>UBS<br>Verizon |

**USA**

| Name | Position | Organisation |
|---|---|---|
| Josh Harris | Director of Policy | TRUSTe |
| Joe Alhadeff | Vice President, Global Public Policy & Chief Privacy Officer | Oracle |
| Hilary Wandall | AVP, Compliance and Chief Privacy Officer | Merck |
| Brendan Lynch | Chief Privacy Officer | Microsoft |

**CANADA**

| Name | Position | Organisation |
|---|---|---|
| Anick Fortin-Cousens | Program Director - Corporate Privacy Office & Privacy Officer Canada, LA, MEA | IBM |

**MEXICO**

| Name | Position | Organisation |
|---|---|---|
| Isabel Davara | Lawyer | Davara Abogados, S.C |
| Jacobo Esquenazi | Global Privacy Strategist | HP Inc. |

## 8.3 Regulator

**JAPAN**

| Name | Position | Organisation |
|---|---|---|
| Masao Horibe | Chairman | Personal Information Protection Commission |
| Chihiro Irie | Chief of International and Law Affairs subsection, General Affairs Division, Secretariat | Personal Information Protection Commission |
| Maiko Kawano | Specialist for International and Legal Affairs | Personal Information Protection Commission |
| Hirokazu Yamasaki | Deputy Director (International and Legal Affairs) | Personal Information Protection Commission |

**SINGAPORE**

| Name | Position | Organisation |
|---|---|---|
| Evelyn Goh | Director, Communications, Planning & Policy | Personal Data Protection Commission |
| Valeriane Toon | Senior Assistant Director, Communications, Outreach & International | Personal Data Protection Commission |
| Melanie Yip | Manager, Policy | Personal Data Protection Commission |
| Su-Anne Chen | Assistant Chief Counsel | Personal Data Protection Commission |

**USA**

| Name | Position | Organisation |
|---|---|---|
| Melinda Claybough | Counsel for International Consumer Protection | Federal Trade Commission |

No regulator representatives were available from Canada or Mexico.

# 9. Appendix 3 – About the Authors

**Annelies Moens** is Lead author of this Report. She is currently the Deputy Managing Director of Information Integrity Solutions Pty Ltd (IIS), having commenced as Head of Sales and Operations in 2012. Annelies is responsible for driving global business growth and consolidating company operations. She provides strategic privacy advice and engages with clients to deliver a privacy suite of services. Annelies represents IIS at major local and international events.

Annelies co-founded the International Association of Privacy Professionals (IAPP) in Australia and New Zealand in 2008, a membership organisation for privacy professionals in the region. She is a Past President, having previously held roles as President, Vice-President and Treasurer. She is an IAPP Certified Information Privacy Professional (Information Technology).

Annelies has over 15 years of experience in managing complex sales and legal functions predominately in privacy and related fields. She also spent 4-5 years working with the Australian privacy regulator. She has an MBA in General International Management (distinction) from the Vlerick Business School in Belgium, a Bachelor of Laws (Hons 1) and Bachelors of Science and Arts (majoring in computer science) from the University of Queensland and a Diploma in Fundraising Management from the Fundraising Institute of Australia. She is a Fellow of the Australian Institute of Company Directors.

### History of work with APEC on privacy and data protection

Most recently prior to this Report, in mid November 2015 Annelies spoke to Australian businesses on the practical ways in which the CBPR System could be implemented in Australia and enforced by a privacy enforcement authority. This was based on her work as co-expert with Malcolm Crompton on the Impediment Analysis of Australia joining the CBPR System, funded through the APEC MYP, entitled *Report for APEC – Australia – Phase 1 – CBPR – Impediment Analysis* (16 July 2014). This was reported on and presented at the APEC data-privacy subgroup meeting in Beijing, China in August 2014.

Annelies was selected by the Australian Government and Standards Australia to be a keynote speaker at an APEC Harmonisation of Standards Project Workshop on 4 November 2015 for small and medium businesses in APEC and APEC standards bodies. She spoke on 'Best Practice in Cross-Border Data Flows' in which she explained the existence of the CBPR System which the standards bodies were not aware of.

In August 2015, Annelies presented on the benefits of CBPR to business at a satellite event of the data privacy subgroup (SOM III) meetings in Cebu, the Philippines. Annelies also presented a paper (finalised in January 2015) to the APEC Business Advisory Council in Seattle, USA in July 2014 which focused on data stewardship and best practice principles in cross-border data flows. Annelies was also involved in the completion of the first published work on the comparison between BCR and CBPR in September 2013, prior to the publication of the official referential.

**Malcolm Crompton** is founder and Managing Director of Information Integrity Solutions Pty Ltd (IIS), a global consultancy based in the Asia Pacific, specialising in data protection and privacy strategies. IIS assists companies increase business value and customer trust and ensures government meets the high standards expected in the handling of personal information.

Malcolm is a Director and co-founder of the International Association of Privacy Professionals Australia New Zealand (iappANZ), an affiliate of the International Association of Privacy Professionals (IAPP). He was founding President of iappANZ in 2008, a Director of IAPP from 2007 to 2011 and is an IAPP Certified Information Privacy Professional. Malcolm's global reputation and expertise in privacy was recognised when IAPP honoured Malcolm with the 2012 Privacy Leadership Award in Washington DC.

As Australia's Privacy Commissioner from 1999 to 2004, Malcolm led the implementation of the first across the board private sector privacy law in Australia. Through IIS, Malcolm has advised the Asia-Pacific Economic Cooperation forum (APEC) regularly on implementation of the APEC privacy framework from the very beginning. He has also consulted to the Organisation for Economic Cooperation and Development (OECD) and a wide range of industry sectors, including, technology and telecommunications, health, banking, finance, credit reporting and insurance, education, professional services, transport and parcel services, mining and manufacturing, travel and retail and government.

Malcolm is also a Director of Bellberry Limited, a private not-for-profit company which provides privacy and health ethics advisory services, is Chairman and co-founder of PRAXIS Australia Limited, a private not-for-profit company which offers training and education in ethical practices in medical research and is a Fellow of the Australian Institute of Company Directors.

Between 1996 and 1999, Malcolm was Manager of Government Affairs for AMP Ltd. In the previous 20 years, Malcolm held senior executive positions in the Federal Department of Finance, served as both a superannuation scheme trustee and scheme founder and worked in the Transport and Health portfolios. Malcolm has degrees in Chemistry and Economics and was awarded the inaugural Chancellor's Medal for distinguished contribution to the Australian National University.

### History of work with APEC on privacy and data protection

Malcolm's contribution to the development and implementation of the APEC privacy framework commenced in 2004 when he attended the Data Privacy Subgroup meeting in Santiago, Chile in February as Privacy Commissioner. He has attended most of the meetings of the APEC Data Privacy Subgroup since then as part of the Australian delegation or as an invited guest, as well as a number of the meetings of the eCommerce Steering Group (ECSG).

Since 2004 Malcolm has:

- Served as special adviser to the Chair of the Data Privacy Subgroup (2004 and 2005)
- Served as consultant to APEC and organised the first ever APEC Privacy Implementation Seminar in Hong Kong in June 2005 in association with the Privacy Commissioner for Personal Data of Hong Kong
- Served as consultant to APEC and organised the Second APEC Privacy Implementation Seminar in Gyeongju, Korea. These seminars laid down the model that has been used almost every year since for the Data Privacy Subgroup Technical Assistance workshops
- Participated as privacy advisor in workshops to develop the Regional Movement List (RML) system, including meetings in Korea and New Zealand in 2005
- Presented the opening Keynote speech to the APEC Symposium on Information Privacy Protection in E-Government and E-Commerce in Hanoi, Vietnam in 2006
- Served as consultant to APEC and the Attorney-General's Department on the implementation of the APEC Privacy Framework for the Australian APEC year, 2007; organised the Technical Assistance Seminars in Cairns and Canberra and wrote the papers that first set out the eight main components of the Pathfinder project that has since developed the Cross-border Privacy Enforcement Arrangement (PEA) and the Cross Border Privacy Rule system (CBPR)
- Participated in the development of the CBPR system and in Data Privacy Subgroup formal and informal meetings as the CBPR systems was developed.
- One of two experts (the other Annelies Moens) involved in the Impediment Analysis of Australia joining the CBPR System, funded through the APEC MYP, entitled *Report for APEC – Australia – Phase 1 – CBPR – Impediment Analysis* (16 July 2014)

Malcolm has also contributed to the development and understanding of the CBPR system through papers and 'behind the scenes' work in Australia and internationally. Most recently this involved writing and presenting to international audiences *Towards a Truly Global Framework for Personal Information Transfers*, a report comparing the APEC Cross Border Rule System (CBPR) with the EU Binding Corporate Rule system (BCR). He first presented it to the IAPP European Congress in Brussels in December 2013 and in Tokyo in April 2014.

INFORMATION
INTEGRITY
SOLUTIONS

**Information Integrity Solutions Pty Ltd**
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898