



**Asia-Pacific  
Economic Cooperation**

# **Enabling Legal Compliance & Cross-Border Data Transfers with the APEC Cross-Border Privacy Rules (CBPR)**

18 July 2016  
Singapore

Electronic Commerce Steering Group

## Table of Contents

I.	Introduction	3
II.	Welcome and Scene Setting	4
III.	Session I: CBPR Basics – What They Are and How They Work	4
IV.	Session II: From an From an All-APEC Transfer System to a Global Transfer System	5
V.	Session III: A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join	6
VI.	Session IV: A Deep-Dive into the Certification Process	7
VII.	Session V: Enforcing the CBPR	8
VIII.	Conclusion	9
IX.	Appendix 1: Workshop Agenda	10
X.	Appendix 2: Speakers	14
XI.	Appendix 3: Workshop Participants	22
XII.	Appendix 4: Workshop Powerpoint	26
XIII.	Appendix 5: Information Integrity Solutions Report for APEC: <i>Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System</i>	27

*An APEC & CIPL workshop for information controllers, information processors and regulators in the Asia-Pacific region.*

**Enabling Legal Compliance & Cross-Border Data Transfers with the APEC Cross-Border Privacy Rules (CBPR)**

Monday, 18 July 2016  
Singapore

**Workshop Report**

**I. Introduction**

Information privacy and the free flow of data in the Asia-Pacific region have been one of APEC's priorities for more than a decade now. In 2005, APEC, through the Electronic Commerce Steering Group (ECSG) and its Data Privacy Subgroup (DPS), completed the APEC Privacy Framework (Framework) that set forth nine high-level privacy principles and guidance on domestic and international implementation. The Framework included a mandate for the APEC Member Economies to develop a cross-border privacy rules system for businesses to "facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers."<sup>1</sup>

After a multi-year, multi-stakeholder negotiation process, the 21 APEC Member Economies endorsed the "APEC Cross-Border Privacy Rules" or "CBPR" system and began the currently ongoing implementation process across the Member Economies. To participate in the CBPR system, individual Member Economies must meet certain requirements, such as having at least one Privacy Enforcement Authority (PEA) that is able to enforce the CBPR against participating businesses and at least one Accountability Agent (AA) that will review and certify companies under the CBPR before they can participate. If they meet the basic pre-requisites for participation, Member Economies that wish to participate must formally join the CBPR system. Once an economy has joined the CBPR and has designated at least one AA, businesses in that economy may seek CBPR certification from the AA. Once a business is CBPR certified, it must comply with the specific privacy and information security program requirements of the CBPR.

To date, four APEC Economies have joined the CBPR system – the United States, Mexico, Japan and Canada. Other economies are currently considering and taking steps to join the system in the future. Only the United States and Japan so far have designated their AAs – TRUSTe for the US, and JIPDEC for Japan. Both AAs are accepting applications for CBPR participation by businesses. So far, there are about 16 CBPR certified companies and many more in the application pipeline.

---

<sup>1</sup> APEC Privacy Framework, part iv. Implementation, Part B.III.48

In 2015, the APEC Economies also endorsed the APEC Privacy Recognition for Processors (PRP), which is a cross-border privacy code of conduct specifically for information processors that the APEC Economies developed following the completion of the CBPR. To date, no APEC Economy has joined the PRP.

In order to increase awareness and knowledge about the purposes and functioning of the CBPR system among government and private sector stakeholders and to help develop Member Economies' domestic capabilities to implement the CBPR system, APEC has established a multi-year funding project for CBPR capacity-building initiatives (MYP). The 18 July 2016, CBPR workshop in Singapore that is the subject of this Report was organized by the Centre for Information Policy Leadership (CIPL) under the auspices and in furtherance of the MYP. Given that the CBPR and PRP are related and complementary systems, they were both covered at the workshop. (The agenda for the workshop is attached as Appendix 1; the speakers' biographies are attached as Appendix 2).

Approximately 100 participants attended the workshop. (The list of attendees is attached as Appendix 3).

## **II. Welcome and Scene Setting**

**Piet Grillet**, General Counsel of MasterCard Asia Pacific, opened the workshop. The conferencing facilities were graciously provided by MasterCard. Mr. Grillet noted that cross-border data transfers must have the appropriate level of protection and welcomed the development of the CBPR system towards that end.

**Bojana Bellamy**, President of CIPL, added in her welcoming remarks that developing the CBPR and similar accountability systems is particularly important for building bridges in a world of fragmented privacy regimes as well as for creating reliable transfer mechanisms and cross-border privacy protections in APEC and globally.

**Zee Kin Yeong**, Assistant Chief Executive of the Personal Data Protection Commission Singapore (PDPC), discussed the broader context of the CBPR from a Singaporean perspective, noting Singapore's desire to become the first "smart nation" based on innovative and effective use of information. He emphasized that this goal can only be accomplished when information can flow freely and accountably across borders. He noted the importance of building public trust through responsible information management and use practices.

## **III: Session I: CBPR Basics – What They Are and How They Work**

**Markus Heyder**, Vice President and Senior Policy Counselor of CIPL and **Joshua Harris**, Director of Policy at TRUSTe, provided a basic introduction into the CBPR and the PRP to ensure that all participants have a common baseline of understanding for the more in-depth sessions on specific CBPR topics in the afternoon. (All presentations used during the workshop are attached as Appendix 4).



**Zee Kin Yeong**, of the PDPC discussed the PDPC's current deliberations about how Singapore could implement and participate in the CBPR. He commented on the specific potential benefits of the CBPR for Singapore and local businesses as well as addressed some of the legal and other issues that remain to be resolved in terms of Singapore's participation in the system, such as how enforcement and oversight would work.

#### **IV. Session II: From an All-APEC Transfer System to a Global Transfer System**

**Jacobo Esquenazi**, Global Privacy Strategist at HP, Inc., moderated a panel designed to cover a range of issues relating to the implementation and growth of the CBPR and PRP systems within the APEC region and connecting the APEC systems to non-APEC cross-border transfer systems, such as the European Union's Binding Corporate Rules (BCR). The comments of the panelists and audience signaled widespread interest in growing the CBPR and PRP systems more quickly as well as underlined the importance of making them interoperable with other systems to enable organizations' need for a global solution to global data flows.

**Andrew Flavin**, Policy Advisor, Office of Digital Service Industries, International Trade Administration at the US Department of Commerce, discussed the current state of implementation of the CBPR and PRP within APEC and highlighted some of the recent positive developments that indicate mounting interest among APEC economies to join the CBPR system. He also encouraged APEC economies to make use of the PRP, particularly those economies that have expressed a strong interest in an information processor rules system for APEC due to their significant domestic processing industries. Finally, he discussed the ongoing work between APEC and the EU to streamline dual applications and towards "interoperability" between the CBPR and BCR, such as by creating a common application form, a joint map of materials needed for demonstrating compliance, and a document mapping the BCR for processors to the PRP.

**Bui Thi Thanh Hang**, Vice Head, International Affairs Division, Viet Nam E-commerce and IT Agency (VECITA) of the Ministry of Industry and Trade, described the ongoing CBPR implementation process in Viet Nam as well as the outstanding issues that remain to be resolved in Viet Nam, including the issue of government oversight and enforcement. Viet Nam will hold a CBPR capacity building workshop in October 2016. She noted the substantial benefits Viet Nam sees in the CBPR system.

**Tsuzuri Sakamaki**, Counselor, Personal Information Protection Commission (PPC) Japan, gave an overview over Japan's recent amendments to its privacy law, particularly as they relate to Japan's participation in the CBPR system. Japan will specifically provide for the CBPR to be one of the recognized mechanisms for data transfers under its new regime of data transfer restrictions, whereby data may be transferred to CBPR-certified organizations outside of Japan because they will have demonstrated company-level competency to receive Japanese personal information.

**Hilary Wandall**, AVP, Compliance and CPO for Merck & Co., Inc. discussed the value of accountability-based information management and cross-border transfer systems, such as the CBPR. She also described how her organization's CBPR certification helped streamline its subsequent BCR approval in the EU, thereby validating the importance of the "interoperability" work currently in progress between the EU and APEC.

## **V. Session III: A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join**

**Markus Heyder**, CIPL, moderated a panel designed to provide a close look at the specific advantages and benefits to companies that the CBPR and PRP systems will deliver. The issues touched upon by the panelists included considerations that are relevant for large multinational companies and SMEs. They also commented on how CBPR benefits may differ from jurisdiction to jurisdiction and how a CBPR certification can be leveraged to streamline approval of an organization's BCR in the EU.

**Annelies Moens**, Deputy Managing Director at Information Integrity Solutions, provided the participants with an overview over her recent study of CBPR benefits entitled "Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR system," which provided a detailed analysis of the numerous benefits of the CBPR from the vantage point of the various stakeholders, ranging from governments, businesses and regulators. She emphasized the importance of further awareness-raising related to the CBPR system, as there still appears to be widespread lack of knowledge among stakeholders that might benefit from the CBPR. She also touched on the issue of providing incentives to businesses to seek CBPR certification, especially in jurisdictions that do not yet have data transfer restrictions and where the immediate need for CBPR might, therefore, not be apparent. (A copy of this report is attached as Appendix 5).

**Daisuke Nagasaki**, Deputy Director, International Affairs Office, Commerce and Information Policy Bureau in the Ministry of Economy, Trade and Industry, Japan (METI), described Japan's rationale for joining the CBPR system, noting that the CBPR will be placed under Japan's recently amended Personal Information Protection Act, which will be fully implemented by September 2017, as a tool to prove adequacy at a company level for purposes of cross-border personal data transfers. For that reason, he urged other APEC economies to join the system as well. He also emphasized the function of the CBPR to demonstrate corporate social responsibility on the part of a company.

**Jacobo Esquenazi**, HP, Inc., explained why HP Inc. obtained CBPR certification. Among other reasons, such as the increase in APEC economies that prohibit transfers absent participation in some mechanism such as the CBPR, he noted how they aligned with and enabled HP's information management and use culture that is based more on an accountability model than a liability model. He noted that data must move for business reasons rather than legal reasons. Participating in the CBPR system enables that approach while also enabling stronger privacy protections, particularly when more APEC economies join the CBPR and PRP systems, more

companies become certified, and the APEC transfer systems connect to other non-APEC transfers systems.

**Harvey Jang**, Director, Global Privacy & Data Protection at Cisco described the rationales of Cisco for seeking CBPR certification. The benefits in joining the system included (1) demonstrating legal compliance and accountability; (2) external validation and testing by a third party; (3) global interoperability and consistency; (4) meeting employee and customer expectations; and (5) building and enhancing trust. He also noted competitive differentiation as one of the benefits of CBPR participation.

**Huey Tan**, Senior Privacy Counsel at Apple stressed the importance and tremendous potential of a trust-based data transfer network for APEC and beyond. Noting the cultural affinity between some of the Asian economies and the CBPR's "communal" approach to data protection, he urged APEC economies to more quickly embrace and build-out this system so that it can become a viable mechanism for businesses of all sizes in the region and a stepping stone for a global approach to accountable data transfers.

## **VI. Session IV: A Deep-Dive into the Certification Process**

**Markus Heyder**, CIPL, moderated a panel of Accountability Agents and Privacy Officers on what to expect during the CBPR certification process. The purpose of this panel was to advise interested companies on the particular steps involved in obtaining certification and maintaining it. It was also important to show how the pre-existing level of compliance and privacy preparedness of an organization impacts the CBPR certification process in terms of difficulty and length as well as how the AA can help companies that do not yet have fully formed internal privacy programs in place to develop such programs.

**Josh Harris**, TRUSTe, described TRUSTe's CBPR certification process, explaining in detail the necessary steps starting with the initial application and the types of questions and issues the applicants must address and how they must address them, to the ongoing monitoring requirements and the annual recertification process. He also described how TRUSTe works with the individual applicants to get their internal privacy programs into compliance with the CBPR program requirements.

**Hiromu Yamada**, CBPR Certification Business Office, Japan Institute for Promotion of Digital Economy and Community (JIPDEC), explained JIPDEC's planned CBPR certification process, as JIPDEC has not yet begun to review organizations for participation. JIPDEC has a long history of providing certifications and is in the process of adapting its existing processes for the CBPR context. JIPDEC is ready to receive applications for CBPR certification.

As representatives of two CBPR-certified companies, **Jacobo Esquenazi**, HP, Inc., and **Hilary Wandall**, Merck, discussed their personal experiences with the CBPR certification process. They both stressed how the relative burdensomeness of this process depends on how advanced an organization is in terms of having a comprehensive accountability-based information management and privacy infrastructure in place already. Given the significant overlap of

requirements between the CBPR and BCR, they also discussed how being certified or approved under one of these systems can be leveraged for a simpler approval process in the other system.

**Jacobo Esquenazi**, HP, Inc., explained why HP Inc. obtained CBPR certification. Among other reasons, such as the increase in APEC economies that prohibit transfers absent participation in some mechanism such as the CBPR, he noted how they aligned with and enabled HP's information management and use culture that is based more on an accountability model than a liability model. He noted that data must move for business reasons rather than legal reasons. Participating in the CBPR system enables that approach while also enabling stronger privacy protections, particularly when more APEC economies join the CBPR and PRP systems, more companies become certified, and the APEC transfer systems connect to other non-APEC transfers systems.

**Harvey Jang**, Director, Global Privacy & Data Protection at Cisco described the rationales of Cisco for seeking CBPR certification. Harvey noted that the CBPR requirements are consistent with most other privacy frameworks – OECD, FIPs, BCR, GDPR, Privacy Shield, etc. Obtaining CBPR certification was part of validating and getting external recognition for Cisco's privacy and data protection program (Cisco was certified this month). The benefits in joining the system included (1) demonstrating legal compliance and accountability; (2) efficient and cost-effective external assessment and testing by an independent third party; (3) global interoperability and consistency; (4) meeting employee and customer expectations; and (5) building and enhancing trust. He also noted competitive differentiation as one of the benefits of CBPR participation.

**Huey Tan**, Senior Privacy Counsel at Apple stressed the importance and tremendous potential of a trust-based data transfer network for APEC and beyond. Noting the cultural affinity between some of the Asian economies and the CBPR's "communal" approach to data protection, he urged APEC economies to more quickly embrace and build-out this system so that it can become a viable mechanism for businesses of all sizes in the region and a stepping stone for a global approach to accountable data transfers.

## **VII. Session V: Enforcing the CBPR**

**Bojana Bellamy**, CIPL, moderated a session on the enforcement structure behind the CBPR system, including the system that APEC privacy enforcement authorities have created to cooperate with each other across the different APEC jurisdictions. The purpose of this panel was also to highlight the importance of robust enforcement, including addressing false CBPR claims in an appropriate and consistent way through effective governance of the CBPR system to maintain its credibility to the public and value to the participating businesses and other stakeholders.

**Melinda Claybaugh**, Counsel for International Consumer Protection, Office of International Affairs, US Federal Trade Commission, stressed the importance of strong enforcement to the ultimate success of the CBPR system. She underscored that maintaining the credibility of the CBPR system will be crucial to developing and preserving the public trust in the system, as well as the value of investment of companies that have certified to the CBPR. She also discussed the FTC's first CBPR-related enforcement initiatives against businesses that had falsely claimed in

their privacy policies that they are CBPR-certified. In addition, she noted that the issue of how to combat false claims relating to CBPR certification throughout the CBPR system may have to be further discussed within the APEC DPS to ensure that all participating member economies not only have the capability to enforce the CBPR's substantive program requirements but also to combat false claims associated with the CBPR.

**Andrew Flavin**, US Department of Commerce, described possible ways forward through the DPS, a DPS working group and/or the CBPR Joint Oversight Panel (JOP) with respect to a number of enforcement, complaint-handling and dispute resolution-related issues that could be further improved and streamlined. For example, he discussed how it is in all stakeholders' interest to ensure that consumers have an effective and centralized mechanism to log complaints and suggested that the current mechanism found on the CBPR website, [www.cbprs.org](http://www.cbprs.org), might be further refined and improved. Both panelists emphasized the utmost importance of addressing these issues at the early stages of CBPR implementation to avoid bigger problems at a later stage.

## **VIII. Conclusion**

By all accounts, the CBPR workshop appeared a success in terms of wide participation by businesses, governments, regulators and other stakeholders, the wide range of issues covered, and the active engagement by the participants during the panel discussions. A sentiment expressed frequently throughout the day was the need to implement the CBPR system across APEC as quickly as possible to enable its full range of benefits for businesses, governments, privacy authorities and consumers.

Participants also identified a number of key issues that need to be clarified by APEC in the near term, such as, for example, (1) the rules around selecting the relevant jurisdiction for certification for companies (and their subsidiaries) that are active in numerous APEC Member Economies and/or that are headquartered outside of APEC but with significant business operations in APEC, and the precise scope of a CBPR certification in these cases; and (2) how false claims relating to CBPR certification can be enforced against in the various APEC Member Economies.

Finally and importantly, a key message from the workshop was the urgent need for additional public education on the purposes, benefits and workings of the CBPR system. Many stakeholders, including APEC-based governments, regulators, privacy authorities and businesses, are still unsure about key elements of the CBPR/PRP systems and continue to request more user-friendly, easy-to-understand information about these systems to enable their deliberations about whether and how to participate in the CBPR/PRP systems.

## **Appendix 1**

### **Workshop Agenda**

An APEC & CIPL workshop for information controllers, information processors and regulators  
in the Asia-Pacific region

## **ENABLING LEGAL COMPLIANCE & CROSS-BORDER DATA TRANSFERS WITH THE APEC CROSS-BORDER PRIVACY RULES (CBPR)**

MasterCard Singapore  
The Gateway East  
152 Beach Road, 34th floor  
Singapore 189721

Monday, 18 July 2016 | 10:00 – 17:30

### **WORKSHOP AGENDA**

10:00      **Registration for Workshop**

10:30      **Welcome and Scene Setting**

**Piet Grillet**, General Counsel, MasterCard Asia Pacific  
**Bojana Bellamy**, President, Centre for Information Policy Leadership  
**Zee Kin Yeong**, Assistant Chief Executive, Personal Data Protection  
Commission Singapore

10:45      **Session I: CBPR Basics – What They Are and How They Work**

**Moderator: Markus Heyder**, Vice President and Senior Policy Counselor, CIPL  
**Josh Harris**, Director of Policy, TRUSTe  
**Zee Kin Yeong**, Assistant Chief Executive, Personal Data Protection  
Commission Singapore

This session will provide a basic introduction into the CBPR system and its  
corollary for personal information processors (the APEC Privacy Recognition for  
Processors (PRP)). The speakers will leave ample time for Q&A.

12:00      **Lunch (Selection of Gourmet Sandwich Lunch Boxes)**

13:00      **Session II: From an All-APEC Transfer System to a Global Transfer System**

**Moderator: Jacobo Esquenazi**, Global Privacy Strategist, HP, Inc.  
**Andrew Flavin**, Policy Advisor, Office of Digital Service Industries,  
International Trade Administration, US Department of Commerce

**Bui Thi Thanh Hang**, Vice Head, International Affairs Division, Viet Nam E-commerce and IT Agency (VECITA), Ministry of Industry and Trade  
**Tsuzuri Sakamaki**, Counselor, International Policy and Legal Affairs, Personal Information Protection Commission (PPC) Japan  
**Hilary Wandall**, AVP, Compliance and CPO, Merck & Co., Inc.

This session will give an overview over the work that is being done to grow the APEC CBPR system within the APEC region and to build and streamline “dual certification” processes under the CBPR and EU Binding Corporate Rules (BCR). The speakers will leave ample time for Q&A.

14:00 **Session III: A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join**

**Moderator: Markus Heyder**, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership  
**Jacobo Esquenazi**, Global Privacy Strategist, HP, Inc.  
**Harvey Jang**, Director, Global Privacy & Data Protection, Cisco  
**Annelies Moens**, Deputy Managing Director, Information Integrity Solutions  
**Daisuke Nagasaki**, Deputy Director, International Affairs Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan (METI)  
**Huey Tan**, Senior Privacy Counsel, Apple

This session will provide a close look at the advantages and benefits to companies that CBPR will deliver. The panel will specifically address the different issues and considerations that are relevant for large multinational companies and SMEs, and will discuss how CBPR benefits may differ from jurisdiction to jurisdiction and how a CBPR certification can be leveraged to streamline approval of an organisations Binding Corporate Rules in the EU. The speakers will leave ample time for Q&A.

15:15 **Break (Coffee, Tea and Refreshments)**

15:45 **Session IV: A Deep-Dive into the Certification Process**

**Moderator: Markus Heyder**, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership  
**Jacobo Esquenazi**, Global Privacy Strategist, HP, Inc.  
**Josh Harris**, Director of Policy, TRUSTe  
**Hiromu Yamada**, Japan Institute for Promotion of Digital Economy and Community (JIPDEC)  
**Hilary Wandall**, AVP, Compliance and CPO, Merck & Co., Inc.



Accountability Agents and Privacy Officers describe what to expect during the certification process. The speakers will leave ample time for Q&A.

17:00

### **Session V: Enforcing the CBPR**

**Moderator: Bojana Bellamy**, President, Centre for Information Policy Leadership

**Melinda Claybaugh**, Counsel for International Consumer Protection, Office of International Affairs, US Federal Trade Commission

**Andrew Flavin**, Policy Advisor, Office of Digital Service Industries, International Trade Administration, US Department of Commerce

This session will address the enforcement structure behind the CBPR system, including the system that APEC privacy enforcement authorities have set up to cooperate with each other across the different APEC jurisdictions. It will also highlight the importance of addressing false CBPR claims in a robust and consistent way through the governance of the CBPR System itself to maintain the credibility and value of the CBPR system.

17:30

### **End of Workshop**

## **Appendix 2**

### **Speakers**

## WORKSHOP SPEAKERS

### BOJANA BELLAMY

Bojana Bellamy is the President of Hunton & Williams LLP's Centre for Information Policy Leadership (CIPL), a preeminent global privacy and security policy think tank located in Washington, DC and London. Bojana brings more than 20 years of experience and deep knowledge of global data privacy and cybersecurity law, compliance and policy. She has a proven industry record in designing strategy, and building and managing data privacy compliance programs.

Prior to joining CIPL, Bojana served for 12 years as the Global Director of Data Privacy at Accenture. In this position, she built and managed a global data privacy team and was responsible for Accenture's data privacy strategy and compliance programs worldwide, with respect to internal operations, and the company's technology, outsourcing and consulting services.

Prior to joining Accenture, Bojana worked for eight years as Principal Consultant with Privacy Laws & Business on data protection consulting and auditing projects for private and public sector clients in the UK and abroad.

Bojana was a Board member of the International Association of Privacy Professionals (IAPP) from 2008-2013, and was elected Chair from 2011-2012. She sits on the Advisory Board of the International Data Privacy Law Journal, participates in many industry groups and is a regular speaker at international privacy and data security conferences.

### MELINDA CLAYBAUGH

Melinda Claybaugh is currently a Counselor for International Consumer Protection with the Office of International Affairs for the Federal Trade Commission. Prior to serving in this capacity, she was a senior staff attorney at the Federal Trade Commission, in the Bureau of Consumer Protection's Division of Privacy and Identity Protection. There, she has investigated and pursued cases involving data security, children's online privacy, and violations of the Fair Credit Reporting Act. Melinda joined the agency in 2006 and served for 7 years in the Division of Enforcement, where she prosecuted cases against defendants operating a variety of scams, including telemarketing fraud, phony auto warranties, and bogus debt collection. Melinda is also a graduate of Wellesley College and New York University's School of Law.

### JACOBO ESQUENAZI

Jacobo Esquenazi was born in Mexico City in 1970. He holds a BA in International Relations from *Universidad de las Americas* Mexico (1990-1994). Also holds an MSc in Development Studies from the London School of Economics and Political Science, UK (2001).

Currently he maintains the position of Global Privacy Strategist in HP Inc. Jacobo manages HP's Privacy strategy in compliance and is responsible for managing HP's Privacy Policies,

Standards, and co-regulatory programs as BCR & CBPR. He also represents HP in several industry and international organizations that work on the issue of Data Protection including participation in APEC and OECD.

He previously held the posts of Americas Privacy Officer and Director of Government Relations Americas for Hewlett-Packard Company before the separation. His responsibilities included analysis and influence of public policy and legislative lobbying. In addition he coordinated globally the issue of Data Privacy within the Government Relations organization closely working with HP's Privacy Office.

Prior to working at HP he held several positions in Mexico's Ministry of Economy with responsibilities on the issues of environment, e-commerce, intellectual property and other trade issues in various multilateral organizations as APEC, OECD and WTO. He was part of the APEC organizing Committee in 2001 when Mexico chaired the APEC meetings.

#### ANDREW FLAVIN

Andrew Flavin is a Policy Advisor in the Office of Digital Services Industries at the U.S. Department of Commerce. In this position, he covers policy issues related to the digital economy in Asia and Latin America including cross-border data flows and privacy. He received his Master's in Public Policy from the University of Maryland with a concentration in international economics and his BA in economics and international relations from Wheaton College.

#### PIET GRILLET

Piet Grillet is currently a General Counsel and LFI Lead for MasterCard Asia Pacific, and has held this position since July 2014. Prior to serving in this capacity, Piet has served as a Group Head and Lead Regional Counsel for MasterCard's Asia Pacific, Middle East, and African regions.

#### BUI THI THANH HANG

Ms. Hang Bui serves as Vice Head of International Affairs Division, Viet Nam E-commerce and IT Agency, Ministry of Industry and Trade. She had previously served as Deputy Director of Viet Nam E-commerce Development Center and also was a member of Viet Nam negotiation team in the area of e-commerce. Her work currently involves in the international cooperation activities serving the e-commerce development and application in private sector. She has also carried out national programs on privacy and consumer protection in e-commerce.

#### JOSH HARRIS

Josh is based in D.C. and as TRUSTe's Policy Director frequently travels to San Francisco, Europe, Latin America and Asia to contribute to work being done by the government and the industry on data privacy interoperability. He also serves as the lead on TRUSTe's APEC Cross Border Privacy Rules certification system to ensure the safe transfer of data across different

locations. Previously, Josh served as Policy Director for Future of Privacy Forum, a Washington, D.C.-based think tank. Before that, Josh was Associate Director in the Office of Technology and Electronic Commerce at the International Trade Administration. Josh has also worked in private practice as an international trade attorney.

In 2004, he was selected to the White House's Presidential Management Fellowship program. In 2008, Josh was recognized with a professional award for his contributions to a Presidential trade initiative. In 2012, Josh received the United States Department of Commerce Gold Medal – the highest award offered by the Department – for his work on the APEC Cross Border Privacy Rules System. From 2011 – 2013, Josh was the Vice-Chair of the Asia Pacific Economic Cooperation's (APEC) Data Privacy Subgroup and Chair of the Cross Border Privacy Rules System's Joint Oversight Panel. Previously, Josh was the Vice-Chair of the American Bar Association's Privacy and Information Security Committee.

Josh received his Juris Doctor from the George Washington University Law School in 2004 and his undergraduate degree from the State University of New York at Geneseo in 2000. Josh was admitted to the Washington, DC bar in 2005.

#### MARKUS HEYDER

Markus Heyder is the Vice President and Senior Policy Counselor of Hunton & Williams LLP's Centre for Information Policy Leadership (CIPL), a preeminent global privacy and security policy think tank located in Washington, DC and London. Markus has extensive experience in global data privacy, information security and consumer protection law and policy. At CIPL he focuses on law and policy issues in the areas of global data flows and cross-border transfer mechanisms, accountable information management in the context of big data, the IoT and other modern information uses, how to enable both privacy protection and innovation, the risk-based approach to privacy, and many other issues.

Prior to joining Hunton & Williams, Markus served for over 10 years as Counsel for International Consumer Protection in the Office of International Affairs at the Federal Trade Commission (FTC), where he worked on global privacy policy issues and represented the FTC in the APEC Electronic Commerce Steering Group and the APEC Data Privacy Subgroup, among other international networks and fora. He also spent and nearly two years in the FTC's Division of Marketing Practices. Prior to joining the FTC, Markus was associated with Lovells (now Hogan Lovells) in Chicago, where he focused on consumer financial services law and financial privacy law.

#### HARVEY JANG

Harvey Jang is Director of Global Privacy and Data Protection for Cisco. He serves as the team lead for privacy and data security related legal matters and is responsible for developing and orchestrating Cisco's global privacy and data protection policies, compliance capabilities, certifications, and accountability frameworks.

Prior to joining Cisco, Harvey was Senior Director, Legal Affairs for McAfee. Part of Intel Security where he was lead counsel for privacy, security, marketing, and antitrust compliance. In this role, he worked closely with engineers and product teams to develop and implement data protection policies and practices, design privacy enhancing products and functionality, and manage legal compliance. Harvey also served as Global Privacy & Security Counsel and team lead for privacy and security legal compliance for Intel. Before Intel, Harvey was the Director of Privacy & Information Management and Chief Privacy & Security Counsel for HP; Senior Compliance Counsel for Symantec; and Litigation Counsel with two prominent international law firms -- Gibson Dunn & Crutcher LLP and O'Melveny & Myers LLP.

He is a member of the Board of Trustees for Bowman International School, serves as an instructor for International Association of Privacy Professionals' privacy credentials (CIPP/US and CIPT), and is a frequent panelist/speaker on a variety of topics related to privacy, security, and information governance.

Harvey earned his B.A., magna cum laude, from UCLA and his J.D., cum laude, from U.C. Hastings College of the Law. He is also a Certified Information Privacy Professional and Certified Information Privacy Technologist (by IAPP), Certified Information Security Manager (by ISACA), and Certified Information Professional (by AIIM).

#### ANNELIES MOENS

Annelies is a highly recognized privacy expert and leader, trusted by business leaders, government agencies and privacy professionals. She has a tremendous depth of experience on privacy issues at the national and international levels. At Information Integrity Solutions Pty Ltd based in Australia, where she is Deputy Managing Director, she is responsible for driving global business growth and consolidating company operations. She provides strategic privacy advice and engages with clients to deliver a suite of privacy services. Annelies was co-founder and a President of the Australian and New Zealand privacy industry membership body (IAPP ANZ).

Over the last 15 years she has held senior leadership roles, including as a Group Manager, External Relations Manager, Chief Privacy Officer and Deputy Director at the Australian privacy regulator. She has an MBA in general international management (distinction) from the Vlerick Business School in Belgium, is a qualified lawyer and has undergraduate degrees in computer science and law (first class honors) from the University of Queensland in Australia. She is a Fellow of the Australian Institute of Company Directors and is a Certified Information Privacy Professional.

#### DAISUKE NAGASAKI

Daisuke Nagasaki is currently the Deputy Director with the International Affairs Office under the Bureau of Commerce and Information Policy for the Ministry of Economy, Trade, and Industry (METI) in Japan. Before serving in this position, he was in charge of promoting the export of nuclear power technologies of Japanese companies, such as Mitsubishi, Hitachi, and Toshiba.

## TSUZURI SAKAMAKI

Tsuzuri Sakamaki is a Counselor for the Personal Information Protection Commission (PPC) in Japan. From 2008 to 2013, Sakamaki was a chief advisor seconded from Japan's Ministry of Finance (MOF) to the State Bank of Viet Nam (SBV) to carry out a technical assistance project to enhance the nation's central banking supervision capacity. During this time, Sakamaki instructed the SBV supervisors in methodologies and techniques regarding CAMELS off-site monitoring of the financial conditions of Vietnamese credit institutions and demonstrated Japan's newly launched bank rating system (FIRST) to help the bank supervisors utilize the financial monitoring results and evaluate the banks' risk management in an efficient and effective manner. Prior to joining Shorenstein APARC, Sakamaki managed an office of MOF to oversee the development, implementation and maintenance of procedures and practices for measuring, monitoring and managing information security risk incurred by the MOF's Local Finance Bureaus' information systems and networks.

## HUEY TAN

Huey Tan is currently the APAC Senior Privacy Counsel for Apple Asia based in Singapore. His legal experience includes privacy and data protection, intellectual property rights, information technology, government affairs, public relations and communication, and legal and regulatory affairs (including law enforcement). Prior to Apple, Huey held senior roles at Accenture (Global Data Privacy and Compliance Lead), Skype (Global Director, APAC government and regulatory affairs), Microsoft (APAC Director of Privacy Compliance) and VP, Business Software Alliance. Huey is a Certified Information Privacy Professional (CIPP) and has a Master's degree in Digital Media from the University of Swansea. He is a PhD candidate at the London School of Economics and Political Science (LSE), and taught Cyberlaw at the LSE's Department of Law. His experience in the APAC region began as an intellectual property lawyer at Baker & McKenzie's Hong Kong office, where he had gained expertise in software copyright issues representing a variety of IP owners, including games and software industry.

## HILARY WANDALL

Hilary Wandall is Associate Vice President, Compliance and Chief Privacy Officer of Merck & Co., Inc., a global health care company that operates in more than 140 countries. She has led the Merck Privacy Office and the company's global privacy program since 2004. In 2013, she also was appointed Divisional Compliance Officer for Merck Animal Health, and is responsible for leading the global ethics and compliance program for this business unit that provides veterinary pharmaceuticals, vaccines, and health management solutions and services. She has broad multi-disciplinary experience in HIV research, genetic and cellular toxicology, internet marketing, corporate law, ethics and compliance, and privacy and data protection. Her career in healthcare spans over 20 years.

Hilary is actively engaged in a broad range of industry and pan-industry outreach and advocacy efforts to address evolving information policy and privacy and data protection policy issues. She is a member of the Board of Directors of the International Association of Privacy Professionals, the Board of Directors of the International Pharmaceutical Privacy Consortium, for which she

previously served as Chair, the Board of Directors of the Foundation for Information Accountability and Governance, and the Future of Privacy Forum Advisory Board. She recently served on the OECD Privacy Experts Group responsible for reviewing the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. She holds a B.S. in Biology from Moravian College, a J.D. and an M.B.A. from Temple University, and a Master of Bioethics from the University of Pennsylvania. She is admitted to practice law in Pennsylvania and New Jersey.

### HIROMU YAMADA

Hiromu Yamada works as director of PrivacyMark secretariat at JIPDEC, Japan. He joined the organization as a researcher of assessment division in 2009, and had been in charge of the general management of PrivacyMark assessors. He also has had the post at CBPR Certification Business Office at JIPDEC since 2015.

### ZEE KIN YEONG

Yeong Zee Kin is a Technology, Media and Telecommunications (TMT) lawyer. Prior to taking up his present appointment as Assistant Chief Executive and Commission Member of the Personal Data Protection Commission, he was Senior State Counsel and Director of Technology Law in the Civil Division of the Attorney-General's Chambers and held a concurrent appointment as Senior Director (Special Projects) in the Legal Services department of the Ministry of Communications and Information. He was also legal advisor to the Smart Nation Program Office and the Cyber Security Agency.

Before this, he was Senior Assistant Registrar and CIO cum CDO of the Supreme Court of Singapore. During his time in the Supreme Court, his administrative responsibilities included (at various times) the management of its registry, statistics unit and CISD. He managed the Supreme Court's Shipping, Intellectual Property, Information Technology and Employment lists. He developed specialized procedures for managing IP cases, eventually collating them and issuing the Supreme Court IP Court Guide. He continues to be engaged in procedural law reform as a member of the Ministry of Law's IP Dispute Resolution Framework Review Committee and the Supreme Court's Civil Justice Commission.

Zee Kin was instrumental in maintaining Singapore's leadership in court technology in electronic filing and introducing online case files. During his time in the Supreme Court, he saw through mid-life enhancements to its first generation Electronic Filing System and managed the development and transition to the current eLitigation system. Additionally, he pushed the boundaries of electronic discovery through the issuance of the Electronic Discovery Practice Directions in 2009 and its revision in 2012, and authoring a number of early decisions in this area. He was also passionate about promoting the use of technology to manage electronic evidence pre-trial and to present electronic evidence during hearings. He implemented the paperless hearing system in the Court of Appeal and pushed out revisions to the Supreme Court Practice Directions to permit the use of presentation slides for oral submissions. He received the Public Administration Medal (Silver) in 2014.



In the area of legal technology, Zee Kin plays an active role in the exploitation of ICT by the legal profession for over a decade. He has been involved in all upgrades to LawNet, the profession's online legal research portal. He is currently a member of the Singapore Academy of Law's Legal Technology Cluster Committee and chair of its Pleadings Selection Committee. He is also active in the promotion of legal education in the area of TMT law. Apart from speaking and publishing in this area, he is a member of the Academy's Technology Law Conference Series core team, the planning committee member managing the program for both its 2011 and 2015 conferences and the editor of the conference publication. He received the Academy's Merit Award in 2013.

He was formerly a partner in Rajah & Tann LLP's iTec (intellectual property, technology, entertainment and communications) practice group and was previously seconded to the Singapore Academy of Law as Assistant Director of LawNet. He commenced his career as Deputy Public Prosecutor and State Counsel with Criminal Justice Division of the Attorney-General's Chambers where he prosecuted a wide range of offenses, including computer and white collar crimes.

## **Appendix 3**

### **Workshop Participants**

An APEC & CIPL workshop for information controllers, information processors and regulators  
in the Asia-Pacific region

## **ENABLING LEGAL COMPLIANCE & CROSS-BORDER DATA TRANSFERS WITH THE APEC CROSS-BORDER PRIVACY RULES (CBPR)**

MasterCard Singapore  
The Gateway East  
152 Beach Road, 34th floor  
Singapore 189721

Monday, 18 July 2016 | 10:00 – 17:30

### **WORKSHOP PARTICIPANTS**

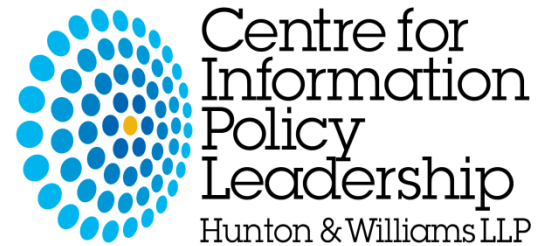
Natividad Alegria	Ministerio de Justicia y Derechos Humanos del Perú
Vivienne Artz	Citi
Tharishni Arumugam	Aon
Kabir Barday	OneTrust
Liam Barker	PayPal
Maria Barriga	Ministerio Secretaría General de la Presidencia, Chile
Bojana Bellamy	Centre for Information Policy Leadership
Susan Bennett	Sibenco Legal & Advisory
Timothy Boettcher	AvePoint, Inc.
Maria Bolshakova	Radio Research and Development Institute (NIIR)
Lisa Cameron	Baker & McKenzie.Wong & Leow
Mei Ling Chan	JPMorgan Chase & Co.
Su-Anne Chen	Singapore Personal Data Protection Commission
Ken Chia	Baker & McKenzie.Wong & Leow
Swee Hoon Chia	Embassy of the United States, Singapore
Alex Chiang	APEC Policy Support Unit
Eric Chung	JPMorgan Chase & Co.
Melinda Claybaugh	US Federal Trade Commission
Will DeVries	Google
Keith Enright	Google
Jacobo Esquenazi	HP, Inc.
Angelene Falk	Australian Office of the Information Commissioner
Andrew Flavin	International Trade Administration, US Department of Commerce
Ben Gerber	DBS Bank
Clarisse Girot	Former Commission nationale de l'informatique et des libertés (CNIL)
Evelyn Goh	Singapore Personal Data Protection Commission

Heather Grell	Apple
Alix Grice	British Telecommunications plc
Christian Grill	Amway
Piet Grillet	MasterCard
Bui Thi Thanh Hang	Viet Nam E-Commerce and IT Agency
Joshua Harris	TRUSTe
Markus Heyder	Centre for Information Policy Leadership
Aya Hiraiwa	Japan Personal Information Protection Commission
Masanori Hirata	Citi
Derek Ho	MasterCard
Kate Holgate	Brunswick Group LLP
Ryan Hollowell	US Department of Commerce
Sheena Jacob	Joyce A. Tan & Partners LLC
Harvey Jang	Cisco Systems, Inc.
Daniel Jin	Centre for Information Policy Leadership
Elaine Khoo	Citi
Ho Seong Kim	Korea Internet & Security Agency
See Khiang Koh	Citi
Helena Koning	ADP
Karina Kudakaeva	Radio Research and Development Institute (NIIR)
Haruhi Kumazawa	Japan Personal Information Protection Commission
Chung Nian Lam	WongPartnership LLP
Eileen Lau	Shell
Travis LeBlanc	Federal Communications Commission
Elaine Lee	Visa
Kate Lee	Google
Chu Lian Lim	Cisco Systems, Inc.
Dennis Low	Huawei
Manuel E. Maisog	Hunton & Williams
Damian Domingo Mapa	Philippines National Privacy Commission
Annelies Moens	Information Integrity Solutions Pty Ltd.
Michael Mudd	Asia Policy Partners LLC
Daisuke Nagasaki	Japan Ministry of Economy, Trade and Industry
Junie Neo	Singapore Personal Data Protection Commission
Dennis Ng	Hong Kong Office of the Privacy Commissioner for Personal Data
Joshua Ngai	Hong Kong Office of the Privacy Commissioner for Personal Data
Quan Nguyen	MasterCard
Van Hai Nguyen	Viet Nam E-Commerce and IT Agency
Leonard Ong	Merck & Co., Inc.
Nicole Oon	UPS
JJ Pan	Acxiom Corporation
Pil Park	Korea Internet & Security Agency
Brendan Pat	Agoda Services Co., Ltd.

Ivy Patdu	Philippines National Privacy Commission
Timothy Pilgrim	Australian Office of the Information Commissioner
Alexander Rogers	APEC Secretariat
Tsuzuri Sakamaki	Japan Personal Information Protection Commission
Merel Schwaanhuysen	Accenture
Yi Lin Seng	Baker & McKenzie.Wong & Leow
Wayne Sim	Sodexo Services Asia Pte Ltd
Dana Simberkoff	AvePoint, Inc.
Eunice Sng	Visa
Blair Stewart	Office of the Privacy Commissioner, New Zealand
Geraldine Stone	Visa
Po Yu Su	Institute for Information Industry (III), Taiwan
Tracy Sua	Singapore Personal Data Protection Commission
Dawn Noeline Tan	Shell
Eu Gene Tan	Accenture
Huey Tan	Apple, Inc.
Louis Tan	Experian
Rowena Mee Hung Tang	Capgemini
Kallie Teo	APEC Secretariat
Valeriane Toon	Singapore Personal Data Protection Commission
Alejandra Vallejos Morales	Ministerio de Economía, Fomento y Reconstrucción de Chile
Adrian Wan	APEC Policy Support Unit
Hilary Wandall	Merck & Co., Inc.
Alan Winters	Teleperformance Group, Inc.
Boris Wojtan	GSMA
Stephen Kai-yi Wong	Hong Kong Office of the Privacy Commissioner for Personal Data
Dick Wong	TRUSTe
Hiromu Yamada	Japan Institute for Promotion of Digital Economy and Community
Toshiki Yano	Google
Karen Yeo	APEC Secretariat
Zee Kin Yeong	Singapore Personal Data Protection Commission
Melanie Yip	Singapore Personal Data Protection Commission
Alicia Young	JPMorgan Chase & Co.
Anais Zavala	Ministerio de Justicia y Derechos Humanos del Perú

## **Appendix 4**

### **Workshop PowerPoint**



# **Enabling Legal Compliance and Cross-Border Data Transfers with the APEC Cross-Border Privacy Rules (CBPR)**

Singapore  
18 July 2016

**No Guest Wi-Fi**

**#CIPLCBPR**

# Welcome and Scene Setting

**Piet Grillet**

General Counsel, MasterCard Asia Pacific

**Bojana Bellamy**

President, Centre for Information Policy Leadership

**Zee Kin Yeong**

Assistant Chief Executive, Personal Data Protection Commission  
Singapore





## Session I

# CBPR Basics – What They Are and How They Work

**Moderator:** Markus Heyder, Vice President and Senior Policy Counselor,  
Centre for Information Policy Leadership

- ❖ Josh Harris, Director of Policy, TRUSTe
- ❖ Zee Kin Yeong, Assistant Chief Executive, PDPC Singapore



## **Objectives**

**Gain an understanding of the functioning of the APEC Cross-Border Privacy Rules (CBPR), the APEC Privacy Recognition for Processors (PRP), how they benefit various stakeholders, and how to obtain the related certification/attestation.**



# APEC Background

## Asia-Pacific Economic Cooperation (APEC)

- 21 economies
- Promotes free trade and economic growth in Asia Pacific
- Many committees and working groups

### Committee for Trade and Investment

### Electronic Commerce Steering Group

### Data Privacy Subgroup (DPS)

The DPS developed the APEC Privacy Framework, the APEC Cross-border Privacy Rules (CBPR) and the APEC Privacy Recognition



# APEC Privacy Framework

## APEC Privacy Framework (2005)

### Privacy Principles:

- preventing harm
- notice
- collection limitation
- uses of personal information
- choice
- integrity of personal information
- security safeguards
- access and correction
- accountability



# APEC Cross-Border Privacy Rules – Basics

## APEC Cross-Border Privacy Rules (2011)

- An enforceable privacy code of conduct for data transfers by information controllers in Asia-Pacific developed by APEC member economies
- Implements the nine APEC Privacy Principles of the APEC Privacy Framework
- Requires third-party certification
- Enforceable



# APEC Cross-Border Privacy Rules – Components of the CBPR System

## Accountability Agents

- Review and certify companies and dispute resolution

## Certified companies

- Seek CBPR certification from Accountability Agents

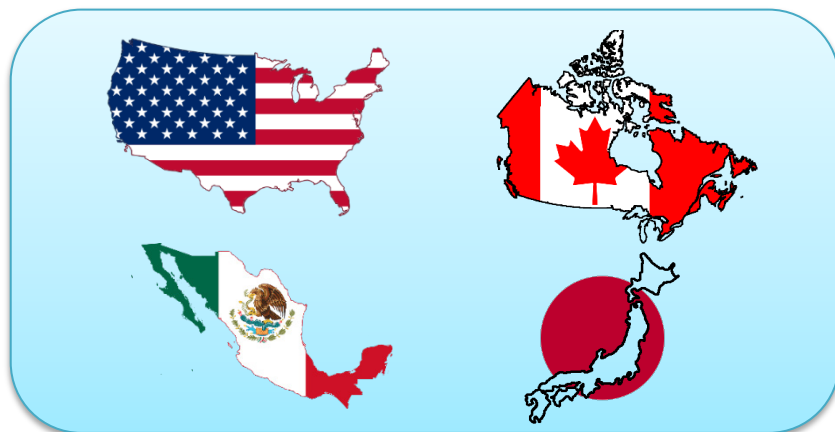
## Privacy Enforcement Authorities (PEAs)

- Enforce CBPRs pursuant to domestic law
- In cross-border matters, cooperate with other PEAs pursuant to the APEC Cross-border Privacy Enforcement Arrangement (CPEA)



# APEC Cross-Border Privacy Rules – Implementation Status

## Participating economies



## Participating Accountability Agents (AAs)



## Certified companies:

Adaptive Insights, Inc.  
Apple Inc.  
Box, Inc.  
Hewlett Packard Enterprise  
Company  
Hightail, Inc.

HP Inc.  
IBM  
Lynda.com, Inc.  
Mashable  
Merck & Co., Inc.  
Rimini Street, Inc.

Saba Software, Inc.  
Workday, Inc.  
Yodlee, Inc.  
Ziff Davis, LLC



Cross Border Privacy Rules System

www.cbprs.org/default.aspx

Google

# CBPRs

CROSS BORDER PRIVACY RULES SYSTEM

A A A

The **APEC Cross Border Privacy Rules (CBPR) system** was developed by participating APEC economies after seeking the views of industry and civil society, to build consumer, business and regulator trust in cross border flows of personal information. The APEC CBPR system requires participating businesses to develop and implement data privacy policies consistent with the [APEC Privacy Framework](#). These policies and practices must be assessed as compliant with the minimum program requirements of the APEC CBPR system by an Accountability Agent (an independent APEC CBPR system recognised public or private sector entity) and be enforceable by law.



## Consumers



## Business



## Accountability Agents



## Government

### Quick Links

- [About CBPR system](#)
- [CBPR system documents](#)
- [Privacy in the APEC region](#)
- [News](#)



**APEC**  
Asia-Pacific  
Economic Cooperation

The [APEC Electronic Commerce Steering Group \(ECSG\)](#) promotes the development and use of electronic commerce. The ECSG also explores how economies may best develop legal, regulatory and policy environments that are predictable, transparent and optimised to enable economies across all levels of development to utilise information and communication technologies to drive economic growth and social development.

[About CBPR system](#) | [Glossary](#) | [Privacy in the APEC region](#) | [News](#) | [Privacy Statement](#) | [Contact us](#)

## APEC Cross-Border Privacy Rules – Website

[www.cbprs.org](http://www.cbprs.org)



# APEC Cross-Border Privacy Rules – Advantages and Benefits

## Consumers

- Enhance privacy protections
- Improve trust through strong rules, and systematic approach towards compliance (AA oversight)
- Streamlined complaint handling
- Co-ordinated government enforcement



# APEC Cross-Border Privacy Rules – Advantages and Benefits

## Government

- At political level – facilitate trade while creating credibility in privacy
- At enforcement level – facilitate cross-border cooperation
- “Front Line” enforcement by Accountability Agent augments resources and extends reach of privacy authorities
- Streamlines investigations due to a comprehensive privacy management program



# APEC Cross-Border Privacy Rules – Advantages and Benefits

## Businesses

- Facilitate legal compliance
- Facilitate cross-border transfers
- Demonstrate accountability
- Create consumer trust
- Create uniformity across the organization



# APEC Privacy Recognition for Processors (PRP)

## Background and Purpose

- Help processors demonstrate ability to implement controller's privacy obligations
- Help small and midsize processors become part of global processing network
- Help controllers identify qualified processors

# APEC Privacy Recognition for Processors (PRP)

## How the PRP works

- Program requirements that are relevant to purpose of processors (e.g. security safeguards and accountability measures)
- APEC CBPR-consistent “baseline requirements”
- Review and recognition process and role of Accountability Agents

# APEC Privacy Recognition for Processors (PRP)

## Enforcement

- Flexible approach, based on national laws
- No backstop enforcement by privacy authority required but possible, unlike the CBPR, where it is required
- Contract between Accountability Agent (AA) and processor
- Government oversight over the AA
- Government oversight via the APEC Data Privacy Subgroup and Joint Oversight Panel (JOP) if AA fails to perform its obligations
- Private right of actions and third-party beneficiary rights for privacy enforcement authorities
- Controllers remain responsible for activities of their processors



# APEC Privacy Recognition for Processors (PRP)

## Status of Implementation

- The PRP program is completed (substantive rules and procedural rules) and ready for use.
- Individual APEC Economies must now join the PRP and designate their PRP Accountability Agents before processors can be recognized.



# Expansion of the CBPR System: PRP and CBPR/BCR Interoperability

## The plans and the trajectory for expansion of the CBPR

- Prospects for creating a CBPR/PRP system with global reach
- Collaborating to increase interoperability between the CBPR and BCR Systems





## **Session I**

# **CBPR Basics – What They Are and How They Work**

**Zee Kin Yeong**

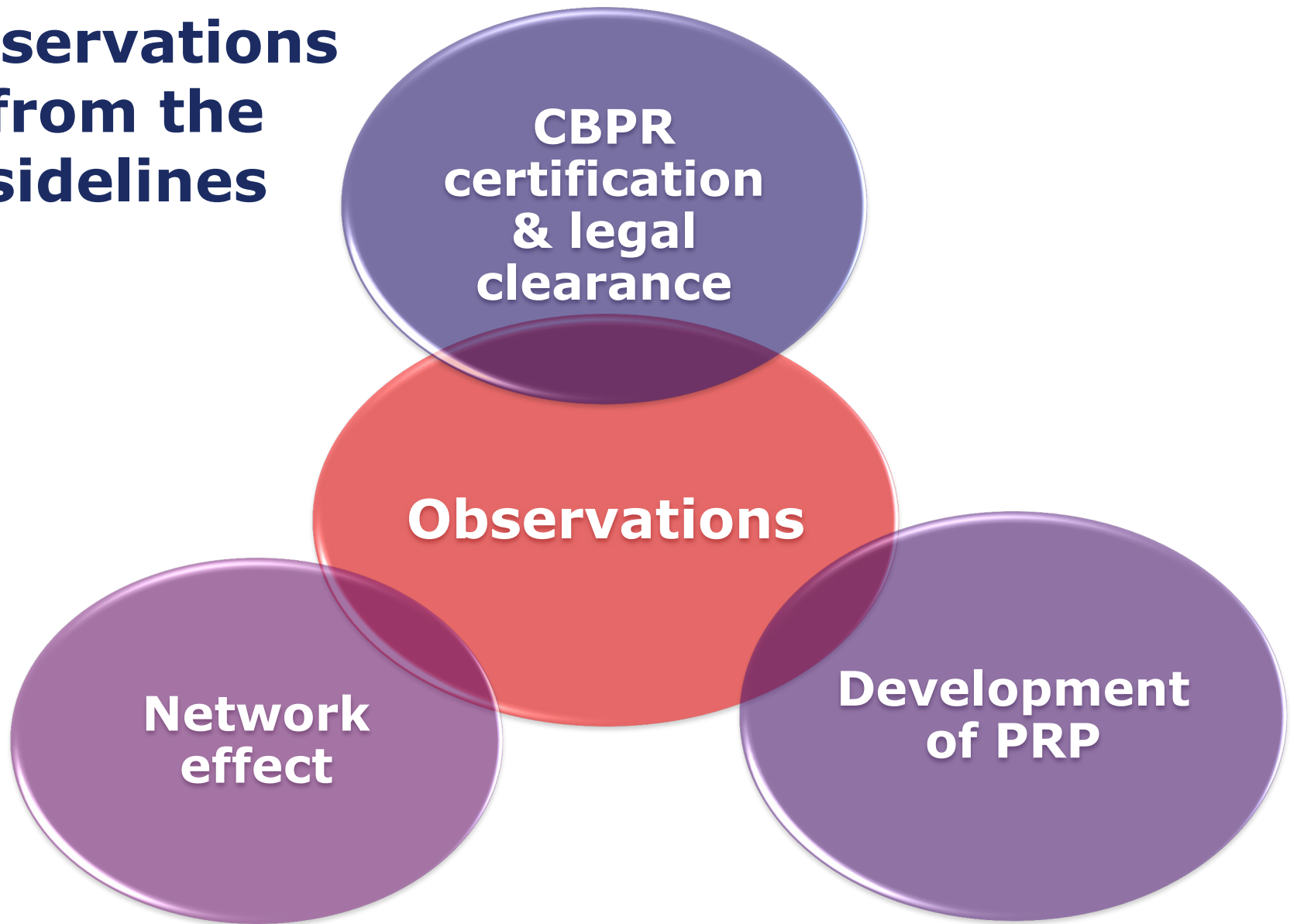
Assistant Chief Executive, PDPC Singapore



**Asia-Pacific  
Economic Cooperation**



# Observations from the sidelines



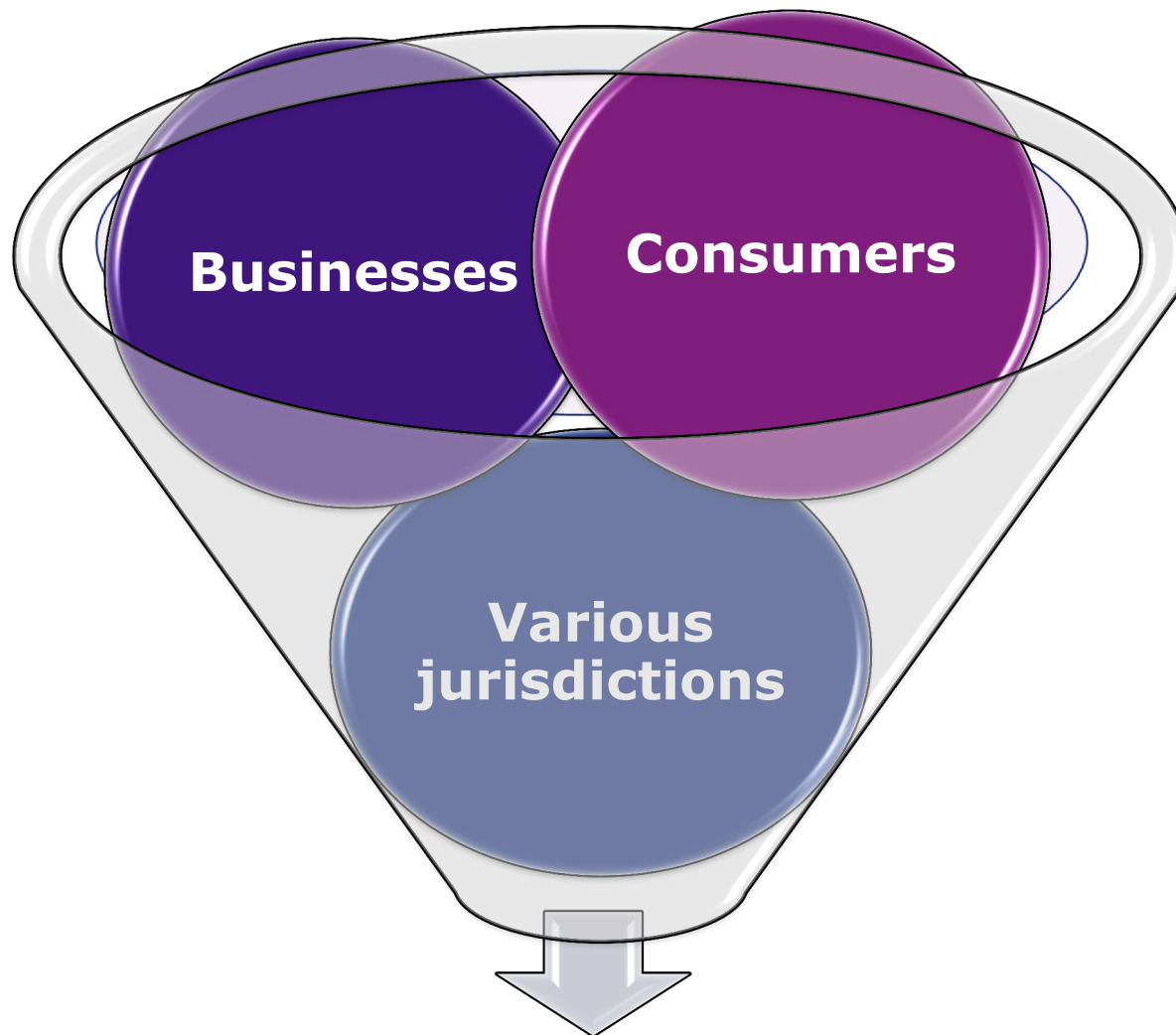
# Exploring CBPR in Singapore's context



Policy &  
legislative  
integration

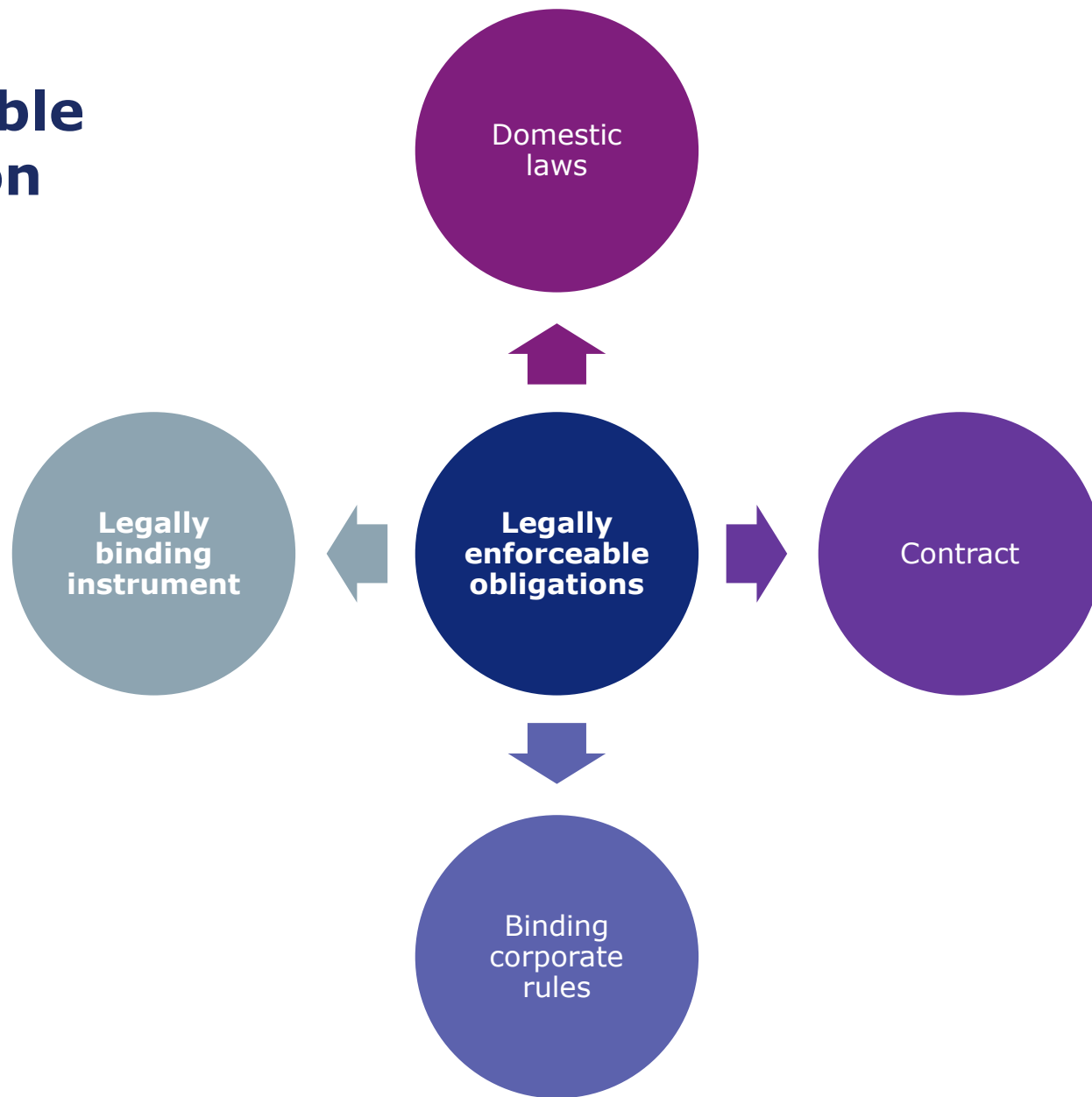
Enforcement  
mechanisms

Compliance  
cost and  
procedures



# Understanding and Learning from stakeholders

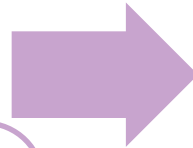
# Ensuring comparable protection



# Potential models: mutually exclusive or progressive integration?

## Self-help

- CBPR certification an objective standard
- Incorporation through contract or binding corporate rules
- Sufficient corporate due diligence



## Tighter coupling

- Recognition of CBPR framework as a legally enforceable obligation
  - Legally binding instrument
  - Specific legislative amendment
- Integration of domestic trust marks with CBPR certification
- Appointment of and regulatory oversight of AA by PDPC



# Summary

## Business

- Recognition by consumers and economies
- Facilitate trade and access to market
- Demand for certification must be sustainable

## Legislation & Policies

- Fulfills Singapore's laws
- Portability of certification

## Enforcement

- Facilitate cross-border enforcement
- Early warning of issues

**END**



# **Lunch**

## **(Boxed Sandwiches in back)**

**Session II begins at 13:00**



**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

## Session II

# From an All-APEC Transfer System to a Global Transfer System

**Moderator:** Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.

- ❖ Andrew Flavin, Policy Advisor, Office of Digital Services Industries, International Trade Administration, US Department of Commerce
- ❖ Bui Thi Thanh Hang, Vice Head, International Affairs Division, Viet Nam E-commerce and IT Agency (VECITA), Ministry of Industry and Trade
- ❖ Tsuzuri Sakamaki, Counselor, International Policy and Legal Affairs , Personal Information Protection Commission (PPC) Japan
- ❖ Hilary Wandall, AVP, Compliance and CPO, Merck & Co., Inc.



## **Session II**

# **From an All-APEC Transfer System to a Global Transfer System**

**Andrew Flavin**

Policy Advisor, Office of Digital Services Industries, International Trade Administration, US Department of Commerce



**Asia-Pacific  
Economic Cooperation**



# Growing the APEC CBPR System



INTERNATIONAL  
**T R A D E**  
ADMINISTRATION

# APEC-EU Interoperability

- Joint Working Team created by the APEC Data Privacy Subgroup (DPS) and the EU Article 29 Working Party
- Designed to reduce administrative burden for companies and strengthen privacy programs
- Could become the basis for interoperability with other non-APEC countries and companies headquartered outside of the APEC region
- Short/Mid-Term Goals:
  - Common Application Form
  - Joint map of materials that must be submitted by companies to demonstrate compliance with CBPR and BCR
  - Map of requirements of EU processor BCR and APEC Privacy Recognition for Processors (PRP)

# APEC Privacy Recognition for Processors (PRP)

- A complement for CBPR System designed for data processors
- Helps data controllers to identify trusted processors and enables processors to demonstrate ability to comply with controllers' requirements
- Functions similarly to CBPR System with some exceptions
  - Does not need to be enforced in all instances through direct backstop enforcement of a privacy enforcement authority
  - Economies are not necessarily required to participate in the Cross Border Privacy Enforcement Agreement (CPEA)
  - Requirements do not cover access and correction or require dispute resolution

## **Session II**

# **From an All-APEC Transfer System to a Global Transfer System**

**Tsuzuri Sakamaki**

Counselor, International Policy and Legal Affairs , Personal Information  
Protection Commission (PPC) Japan



**Asia-Pacific  
Economic Cooperation**



# **Integration of the CBPR System into Japan's Personal Information Protection Regulatory Framework**

---

**Tsuzuri Sakamaki**

July 18 2016

Secretariat

Personal Information Protection Commission

Japan



# What kind of legal groundwork is currently being laid for the CBPR system to be introduced in Japan?

- **Act on the Protection of Personal information (APPI)** was amended
  - Anticipated to become fully effective in around the springtime of **2017**
- **Personal Information Commission (PPC)**
  - Drafting cabinet orders, commission rules and guidelines
  - Planning to hold public consultation in around **August 2016**
- **Cross-border transfer** of personal data
  - **Article 24** of the amended APPI
  - Restriction on transferring personal data to a third party in a foreign country.

# What conditions must be satisfied for transferring personal data to a third party in a foreign country?

- **Article 24** of the amended APPI
- Transfer of personal data to a third party in a foreign country is allowed:
  - a) **Prior consent** from the data subject;
  - b) **Foreign jurisdiction** designated by the PPC as having a data protection regime up to Japanese standards; or,
  - c) **Third-party transferee** upholds data protection standards to be determined by the PPC.
- The **consent** must:
  - Specifically relate to the transfer to that particular recipient
  - Rather than being *general* in nature

## How will the PPC designate a foreign jurisdiction, and what standards will the PPC determine on a transferee?

- **Past Diet deliberations** on the bill to amend the APPI
  - Not adopting increased regulations on business operators
  - Endorse existing treatment that was being conducted appropriately
- Further details will be determined by the PPC rules
  - **Foreign jurisdiction** that the PPC designates
  - **Data protection standards** that a transferee must uphold
- PPC has not planned to designate a foreign country
  - At the time of the **amended APPI**
  - Need to give careful consideration to the current global situation
  - **Many countries both in and outside the APEC region** are reforming their respective legal framework

## Where specifically will the CBPR system be positioned in the upcoming Japan's privacy regulatory regime?

- The PPC has planned to specify standards under **commission rules** or **guidelines** as follows.
  - 1) It is assured by a contract or bylaws that the **third party in a foreign country** will take measure to be taken by a personal information handler in Japan does; and,
  - 2) The **third party in a foreign country** has received certification that it conforms to standards defined by an international framework.
- The PPC will refer specifically to the **APEC CBPR system** in its commission guidelines.

## **Session II**

# **From an All-APEC Transfer System to a Global Transfer System**

**Bui Thi Thanh Hang**

Vice Head, International Affairs Division

Viet Nam E-commerce and IT Agency (VECITA), Ministry of Industry and Trade



**Asia-Pacific  
Economic Cooperation**



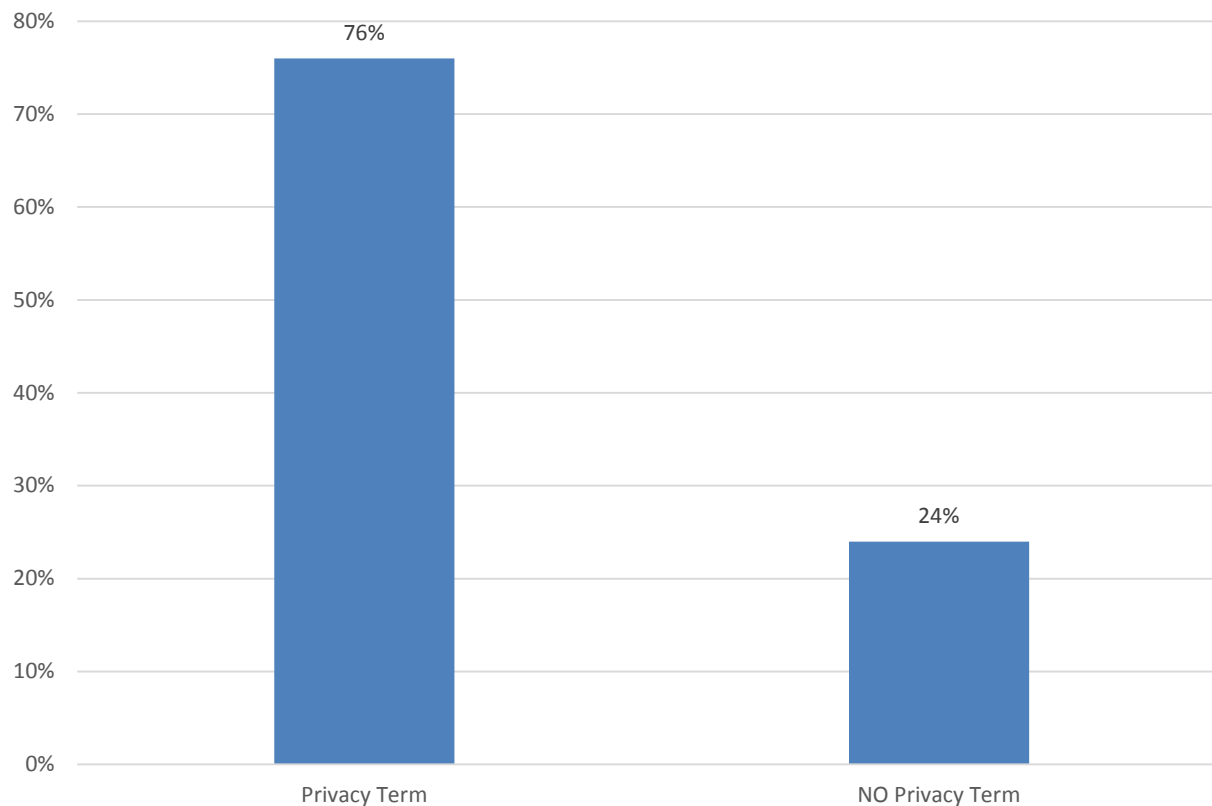
## Viet Nam's intention to CBPRs

- **Government**

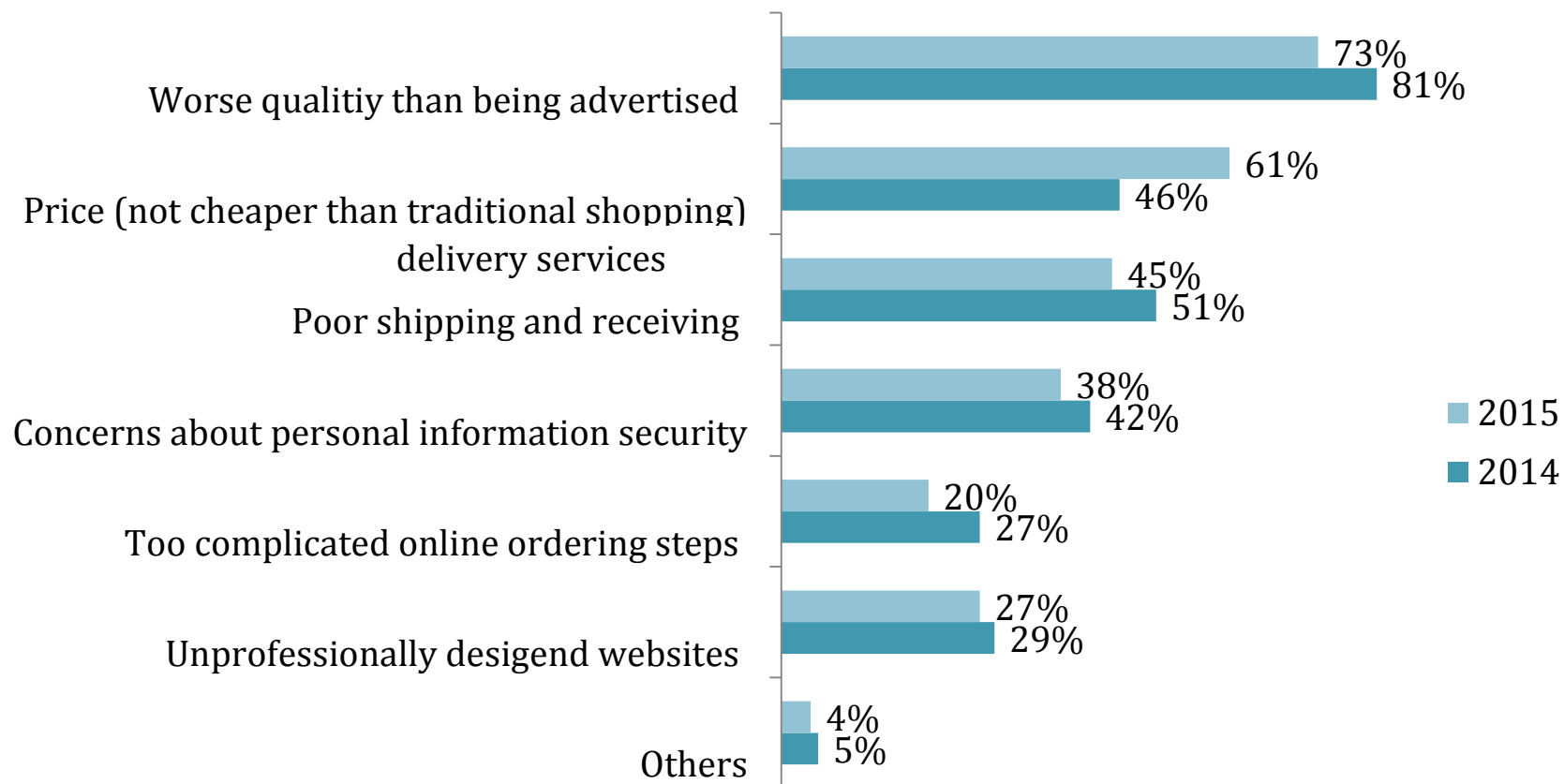
- Established Authority of Information Security in 2014
- Legislation:
  - Law on Information Security: effective on 1 July 2016
  - Decision on orientation, objectives for network information security in the period of 2016-2020 by Prime Minister
  - Decree on Business register for products and services of network information security (draft)



# Businesses



# Consumers – Obstacles for online shopping

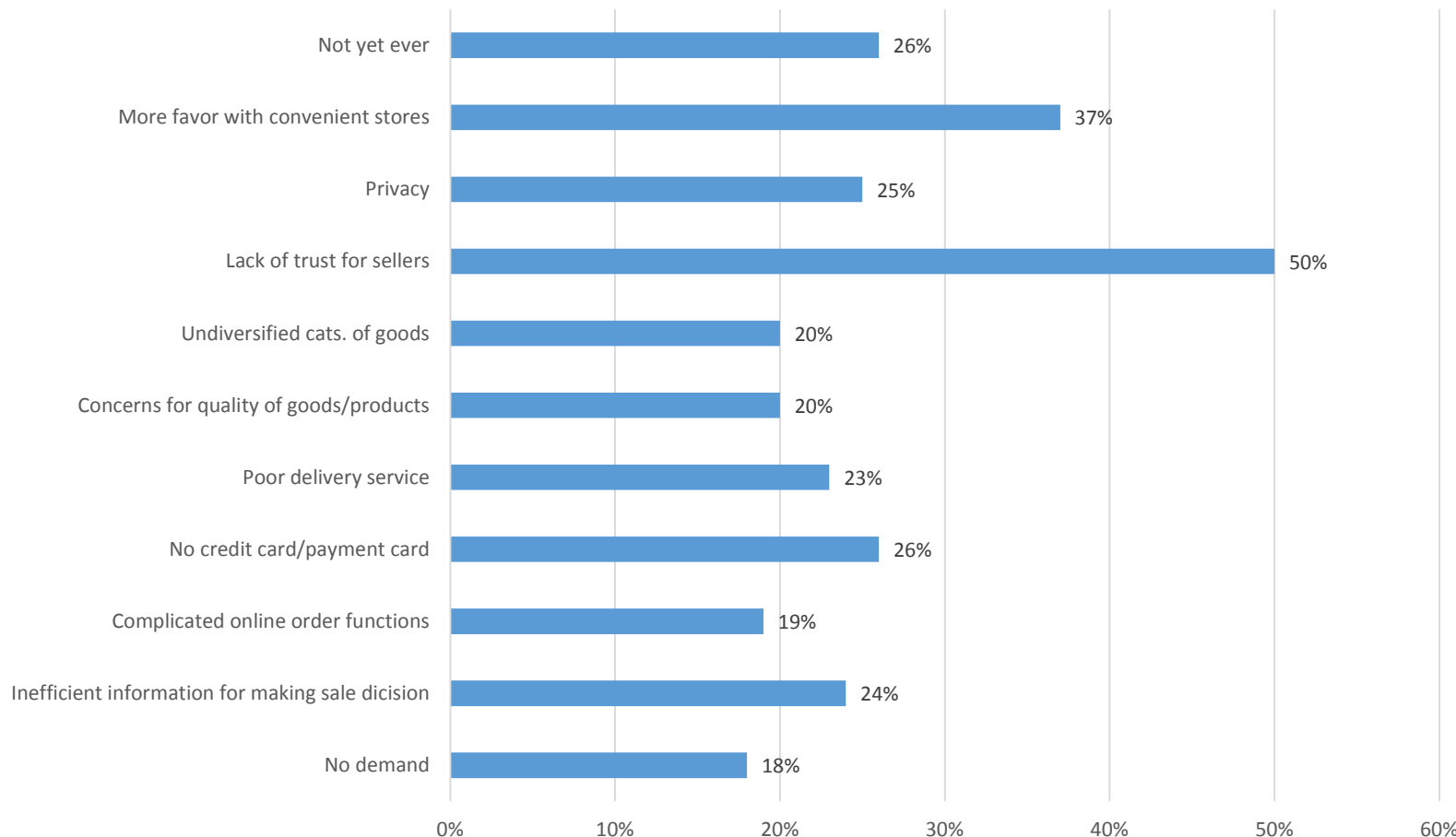


Source : Vecita's survey among 1.000 Internet users in 2015





# Consumers – Reasons for not online shopping



## Viet Nam's intention to CBPRs

- Privacy Regulation
  - Law on Network Information Security
  - Some others laws and decrees
- Privacy Enforcement Authority
  - Authority of Information Security. Ministry of Information and Communication
  - Viet Nam Competition Authority, Ministry of Industry and Trade
  - Viet Nam E-commerce and IT Agency, Ministry of Industry and Trade
- Accountability Agent
  - SafeWeb: 2014



## **Session II**

# **From an All-APEC Transfer System to a Global Transfer System**

**Hilary Wandall**

AVP, Compliance and CPO, Merck & Co., Inc.



**Asia-Pacific  
Economic Cooperation**



# The Evolving Privacy Environment is Complex ...

Our Privacy Program Elements Provide the Foundation for Compliance with Laws and Adherence to Our Values



Our Program is  
Built to Enable Merck to Uphold its  
Global Privacy Commitments and Responsibilities

*Respect*

*Trust*

*Prevent Harm*

*Comply*

**100+ countries with laws addressing 4 types of privacy:**

Information • Bodily • Communications • Location

BCR/ CBPR/  
Privacy  
Shield

Data  
Protection

Breach  
Notification

Health  
Privacy

Workplace  
Privacy

Online/  
Mobile  
Privacy

Telecomm

Location  
Privacy

**Awareness**

**Policies &  
Standards**

**Training**

**Accountability**

**Metrics**

**Culture:** Promote and maintain a corporate culture that respects privacy and protects information about people

**Communications:** Communicate timely information about updates to privacy laws, regulations, rules, guidelines and policy issues

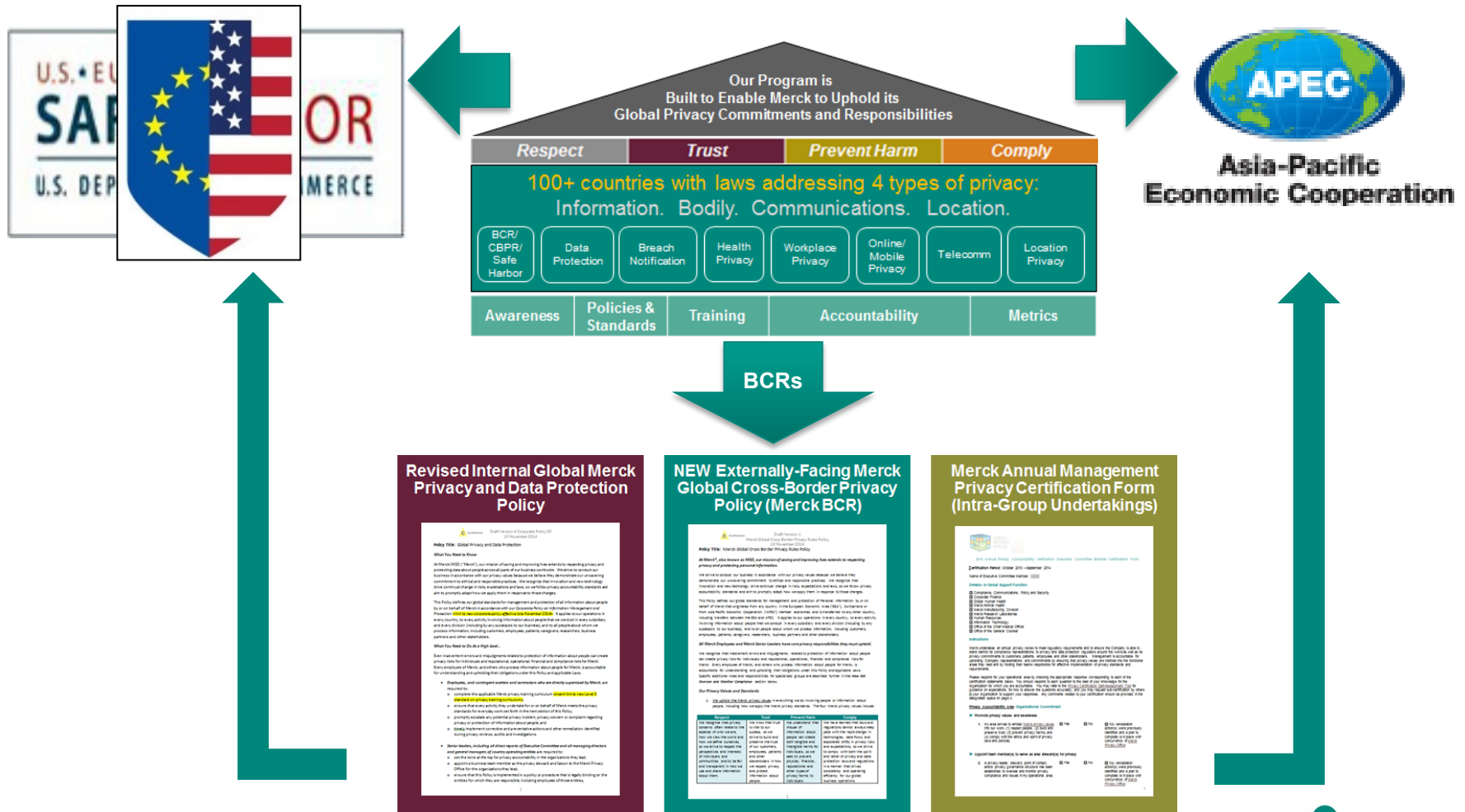
Implement privacy and data protection policies and standards that set forth operational principles and procedures, governance, accountability, incident handling and individual redress

Implement a privacy training curriculum designed to support our “Awareness” and “Policies & Standards” Elements to provide functional privacy knowledge aligned to roles and responsibilities

Demonstrate the effectiveness of our Privacy Program by:  
**Privacy Concept & Design Review (PIA):** Prospectively building and documenting privacy requirements into Merck processes and systems  
**Periodic Assessment:** Verifying privacy and data protection compliance through audits, assessments and investigations  
**Reporting:** Reporting to government authorities as required by law  
**Governance and Annual Certification:** Management acknowledgement and responsibility for assuring that requirements are addressed

**Performance Standards:** Define baseline and target metrics to determine the effectiveness, maturity and risks associated with the Program  
**Continuous Improvement:** Evaluate program effectiveness, maturity and risks and areas for enhancement, improvement and risk mitigation

# Our Approach to Interoperable Frameworks



<http://www.msd.com/privacy/cross-border-privacy-policy/>

# Framework Interoperability Gap Analysis

Privacy Framework Category	Requirements	EU BCRs	APEC CBPRs	Singapore PDPA	Switzerland FADP	Australia APPs	MSD Privacy Program	Referential Sections
Substantive Privacy and Data Protection Standards	Transparency and Fairness	X		Consent		APP Policy		14, 17
	Purpose Limitation	X						10
	Data Quality							11
	Security	X						13, 18
	Access, Correction, Objection	X						15, 16
	Onward Transfer	X						6, 7, 8
	Basis for Processing Personal Data					Collection, Marketing, Government IDs		12, 13
Compliance Verification	National Law Limitations	X						24
	Relationship to National Law							26
	Training							19
	Complaint Handling	X						22
	Audit Program	X						20
Enforceability	Compliance Oversight	X						21
	Internally Binding - Entities	X						3
	Internally Binding - Employees	X						3
	Third Party Beneficiary Rights	X						4
	Liability of Applicant Entity	X						5
	Sufficiency of Applicant Entity Assets	X						5
	Burden of Proof	X						5
	Access to the BCRs	X						4
Scope	Cooperation Duty	X						1, 25
	Geographic Scope	X						2
	Material Scope	X						2
	Entity List	X						2
Other	Purposes of Transfer / Processing	X						2
	Definitions	X						9
	Effective Date and Changes	X						23, 27
Legend								
	Comparable Requirements							
	More Stringent or More Detailed Requirements							
	Requirement on Partially Addressed							
	No Comparable Requirement							
48	X	Merck Case Study: Revisions Requested During BCR Review						

## Session II

# From an All-APEC Transfer System to a Global Transfer System

**Moderator:** Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.

- ❖ Andrew Flavin, Policy Advisor, Office of Digital Services Industries, International Trade Administration, US Department of Commerce
- ❖ Bui Thi Thanh Hang, Vice Head, International Affairs Division, Viet Nam E-commerce and IT Agency (VECITA), Ministry of Industry and Trade
- ❖ Tsuzuri Sakamaki, Counselor, International Policy and Legal Affairs , Personal Information Protection Commission (PPC) Japan
- ❖ Hilary Wandall, AVP, Compliance and CPO, Merck & Co., Inc.



## Session III

# A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join

**Moderator:** Markus Heyder, Vice President and Senior Policy Counselor, CIPL

- ❖ Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.
- ❖ Harvey Jang, Director, Global Privacy & Data Protection, Cisco
- ❖ Annelies Moens, Deputy Managing Director, Information Integrity Solutions
- ❖ Daisuke Nagasaki, Deputy Director, International Affairs Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan (METI)
- ❖ Huey Tan, Senior Privacy Counsel, Apple





# **Potential benefits for APEC economies and businesses joining the CBPR System**

**Annelies Moens, Deputy Managing Director  
Information Integrity Solutions  
APEC & CIPL Workshop, Singapore  
18 July 2016**

# Context

- Value of CBPR depends on:
  - Each economy's underlying domestic law; and
  - Domestic law of current and future trading partners
- Laws (or lack thereof) in relation to cross-border data flows important – generally 3 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 or requirements are met

# Government: Trade benefits



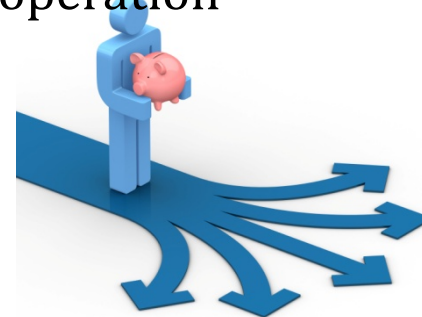
Global trade and economic growth



Increased confidence



International cooperation



Procurement processes

# Government: External stakeholder benefits



Tool to maintain free flow of data with privacy protection



Maintain trust in APEC economies

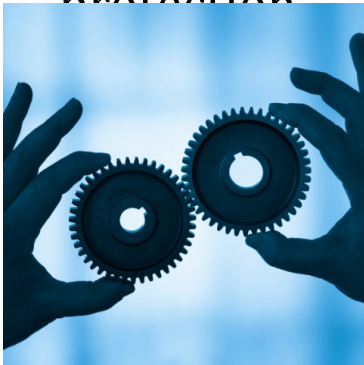


Assurance

# Business: Trade benefits



Appropriate privacy protection



Interoperability



Foreign direct investment

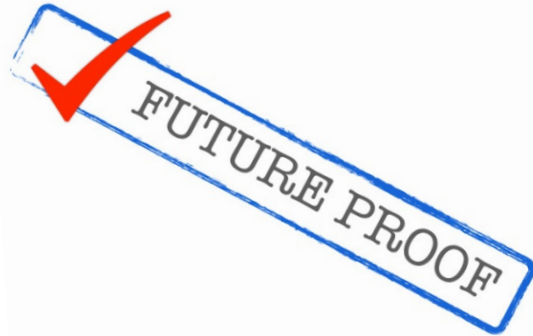


Importing and exporting



Small and medium enterprise

# Business: Internal organisational benefits



One global compliance system



Efficiency and flexibility



Regulatory treatment

# Business: External stakeholder benefits



Assurance



Communication with customers



Good faith and public relations



# Regulator: Internal regulatory benefits



Broadens set of actors that play a role



Enables strategic resource allocation



# Regulator: External regulatory benefits



Assurance



Choice



Raise the benchmark

# Next Steps - Questions

**INFORMATION  
INTEGRITY  
SOLUTIONS**

**Annelies Moens**

Deputy Managing Director

BSc, LLB (Hons), MBA

CIPT, FAICD

Sydney, Australia

Ph: +61 2 8303 2417

Au. M: +61 413 969 753

Int. M: +372 5437 1881

[amoens@iispartners.com](mailto:amoens@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

## **Session III**

# **A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join**

## **Daisuke Nagasaki**

Deputy Director, International Affairs Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan (METI)



**Asia-Pacific  
Economic Cooperation**



# Japan's New Requirement on Cross-Border Transfer of Personal Information

Followings will be required for cross-border transfer of personal information from Japan:

(Basic Rule)

- Acquiring consent from the owner of the personal information

(Exceptional Cases)

- Transfer to a country the personal information protection system of which is confirmed as equivalent with Japanese one by the Commission
- **Transfer to a company having a personal information protection system which is consistent with criteria set by the Commission**

# A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join

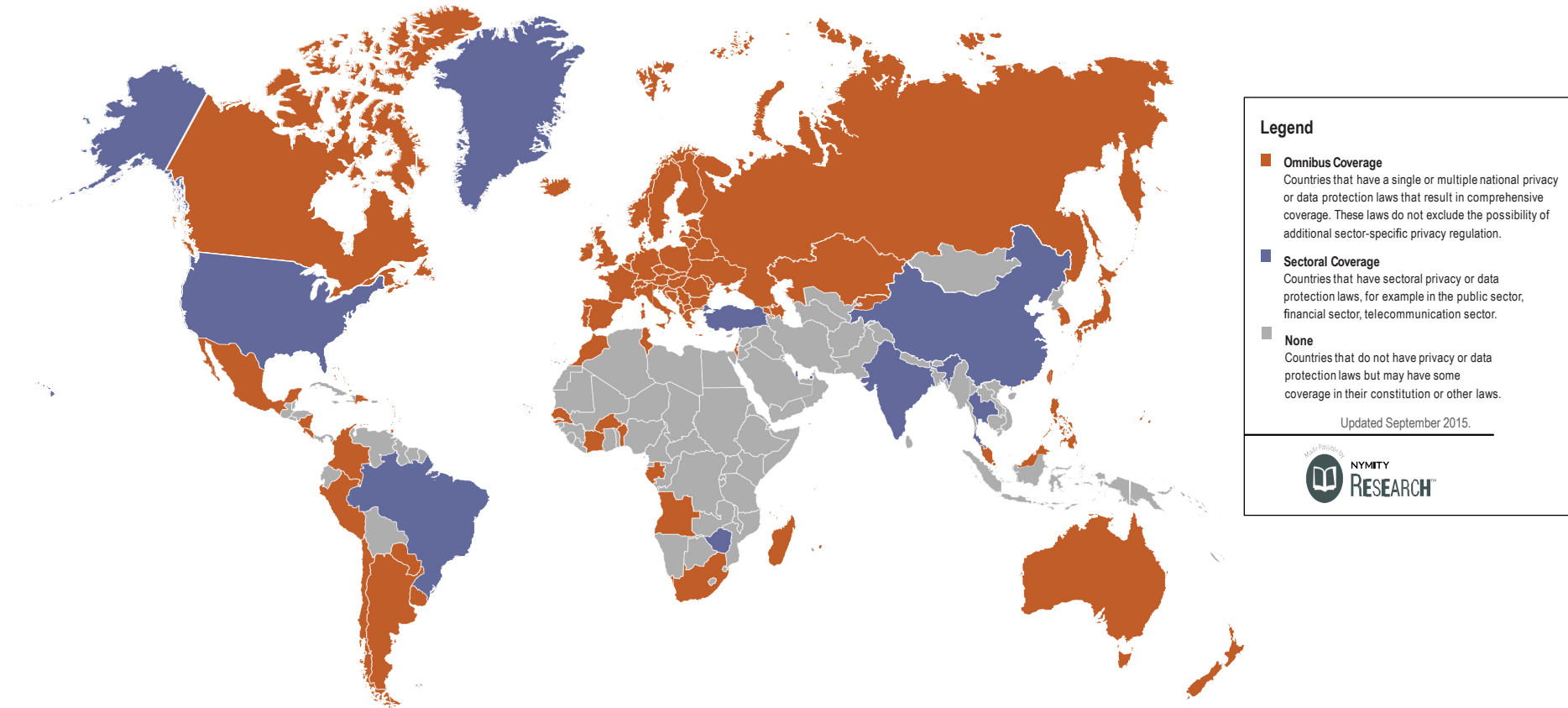
HP's Perspective and Strategy

Jacobo Esquenazi

July 18<sup>th</sup>, 2016



# Sectoral and Omnibus Privacy and Data Protection Laws

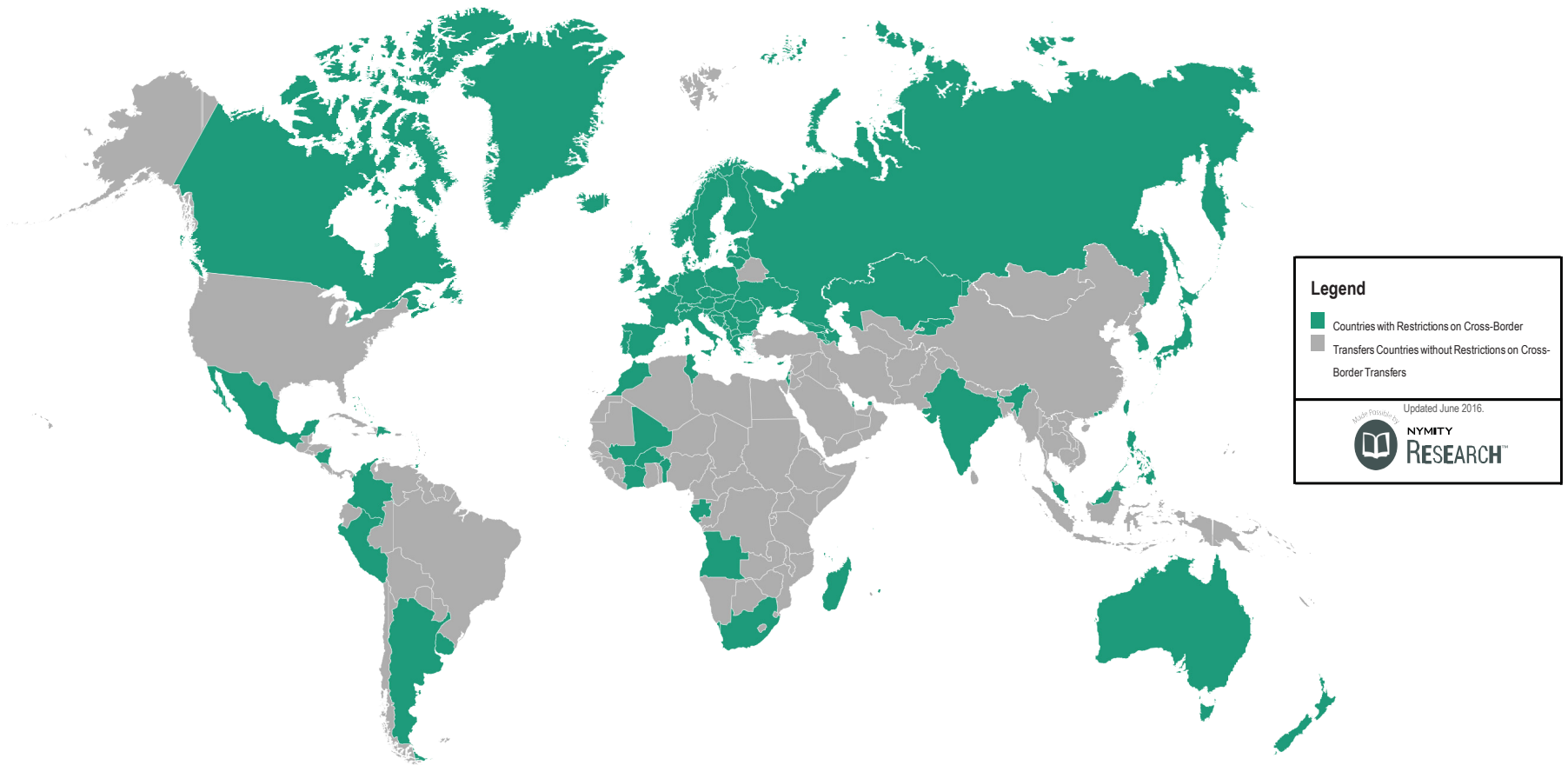


## Omnibus Law Countries

Albania	Belgium	Costa Rica	Finland	Hungary	Kyrgyz Republic	Malta	Norway	Serbia	Sweden	Brazil	St. Vincent & the Grenadines
Andorra	Benin	Cote D'Ivoire	France	Iceland	Latvia	Mauritius	Paraguay	Seychelles	Switzerland	China	Thailand
Angola	Bonaire/St. Eustatius/Saba	Croatia	Gabon	Ireland	Liechtenstein	Mexico	Peru	Singapore	Taiwan	Dubai	Turkey
Argentina	Bosnia & Herzegovina	Curacao	Germany	Isle of Man	Lithuania	Moldova	Philippines	Slovakia	Trinidad &	Greenland	United States
Armenia	Bulgaria	Cyprus	Ghana	Israel	Luxembourg	Monaco	Poland	Slovenia	Tobago	India	Zimbabwe
Australia	Burkina Faso	Czech Republic	Gibraltar	Italy	Macao SAR	Montenegro	Portugal	South Africa	Tunisia	Qatar	
Austria	Canada	Denmark	Greece	Japan	Macedonia	Morocco	Romania	South Korea	Ukraine		
Azerbaijan	Cape Verde	Dominican Republic	Guam	Jersey	Madagascar	Netherlands	Russia	Spain	United Kingdom		
Bahamas	Chile	Estonia	Guernsey	Kazakhstan	Malaysia	New Zealand	San Marino	St. Lucia	Uruguay		
Belarus	Colombia	Faroe Islands	Hong Kong	Kosovo	Mali	Nicaragua	Senegal	St. Maarten			

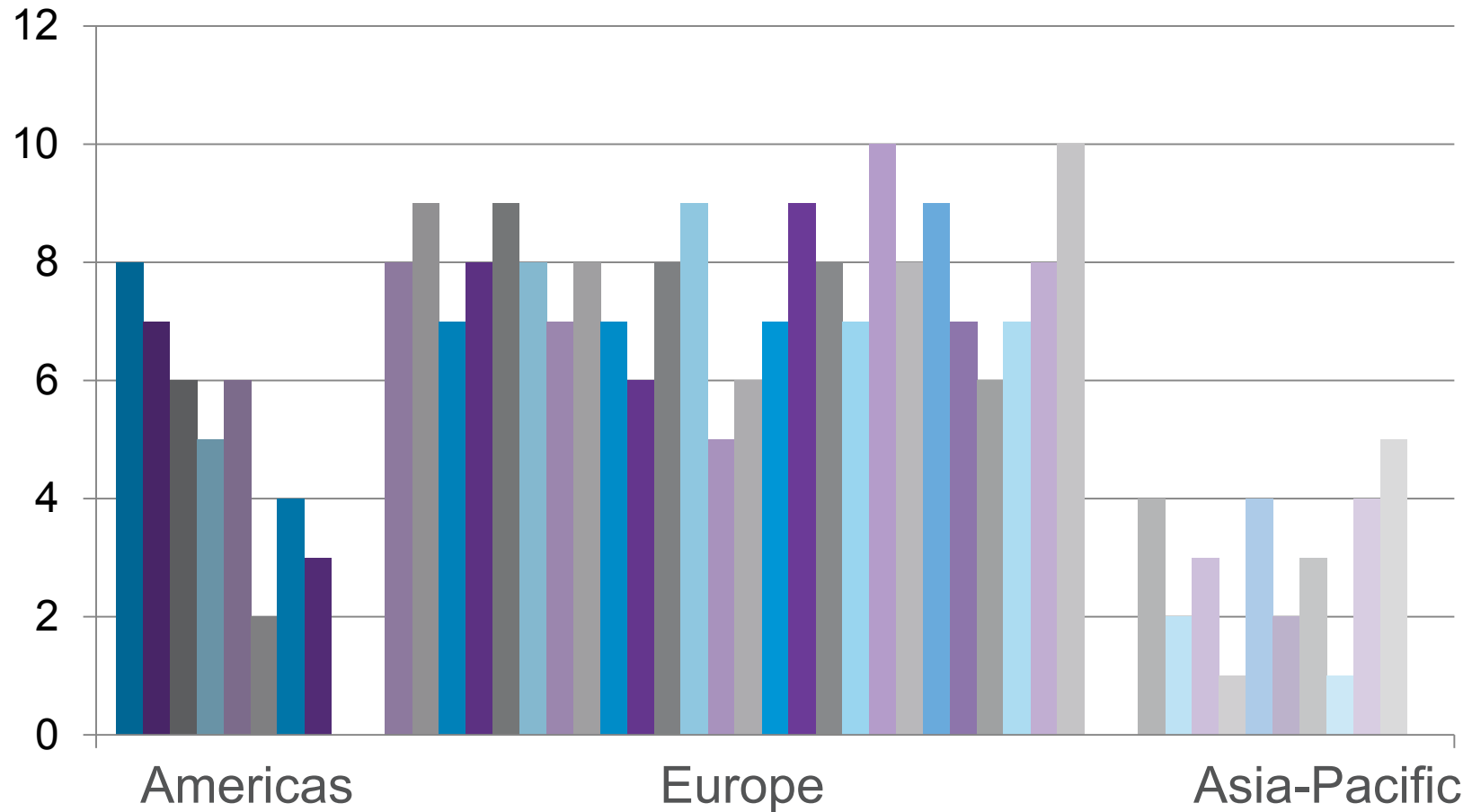
## Sectoral Law Countries

# Countries with Restrictions on Cross-Border Transfers



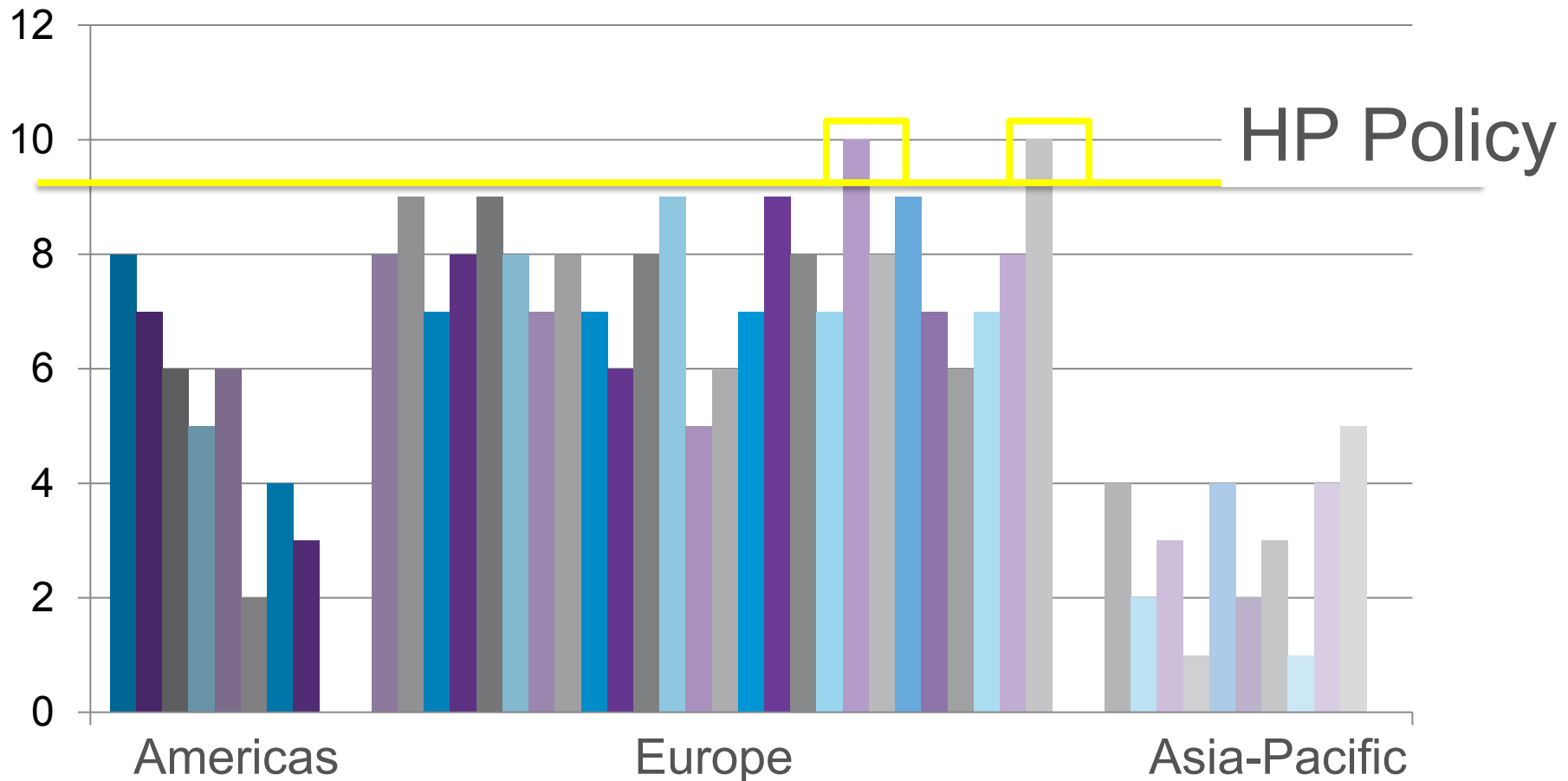
These countries contain restrictions around sending personal data to a third country that does not ensure an adequate level of protection

# Global Privacy Laws





# Global Privacy Laws



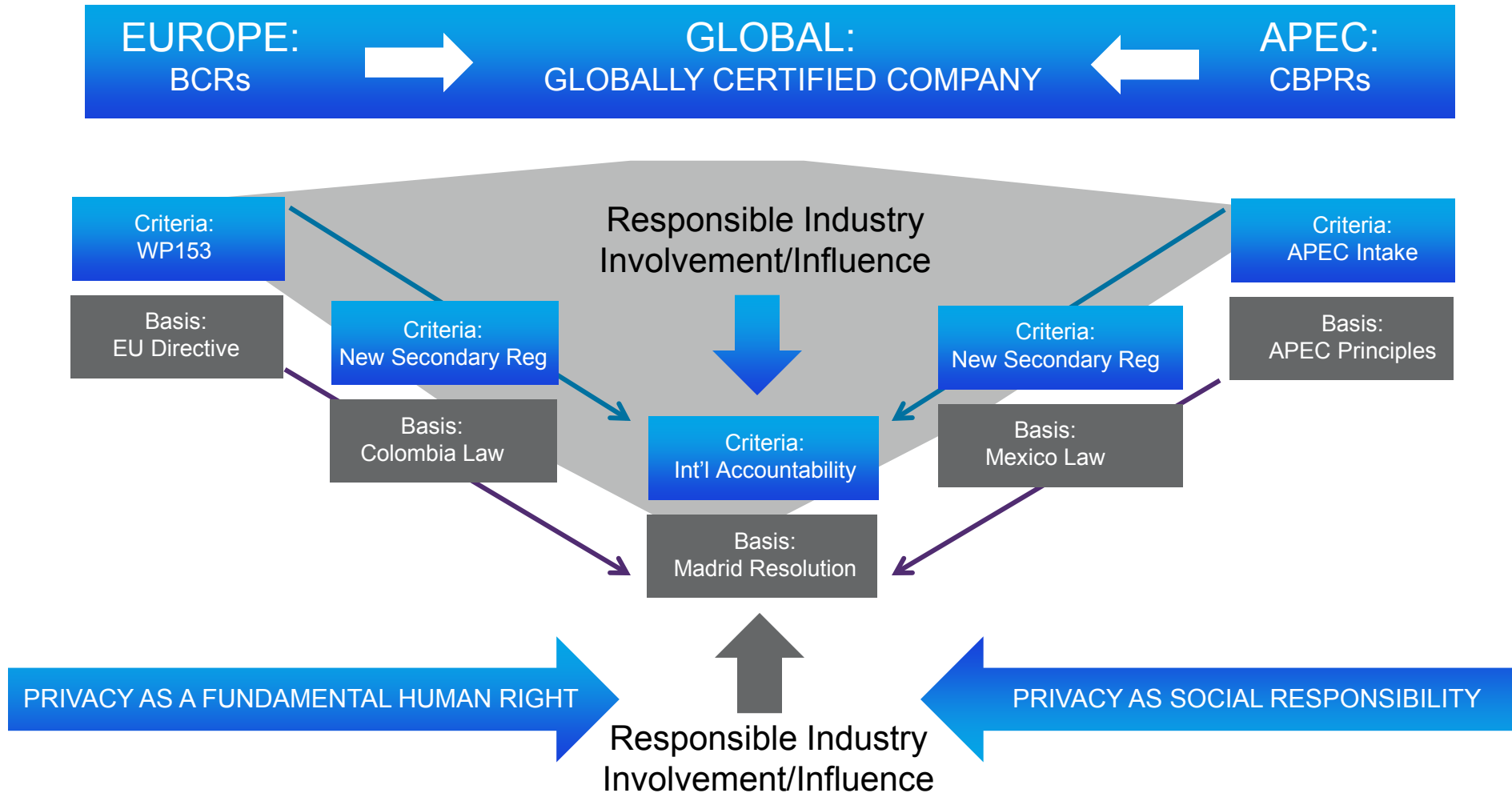
# Global Shift to Accountability

- We are seeing a dramatic change on the part of regulator expectations

LIABILITY	ACCOUNTABILITY
<p>Decisions are made based on technical compliance with local laws and regulations</p> <ul style="list-style-type: none"><li>• Focuses on the minimum standard</li><li>• What is legally defensible</li><li>• Mechanical compliance processes</li></ul>	<p>Decisions are additionally made based on considering concurrent risks and a set of ethics- &amp; value-based criteria beyond liability</p> <ul style="list-style-type: none"><li>• Tie to social and/or company values (ethics)</li><li>• All employees responsible for stewardship of data under their charge (accountability)</li><li>• Demonstrate solid judgment in decisions (risk/harms)</li></ul>



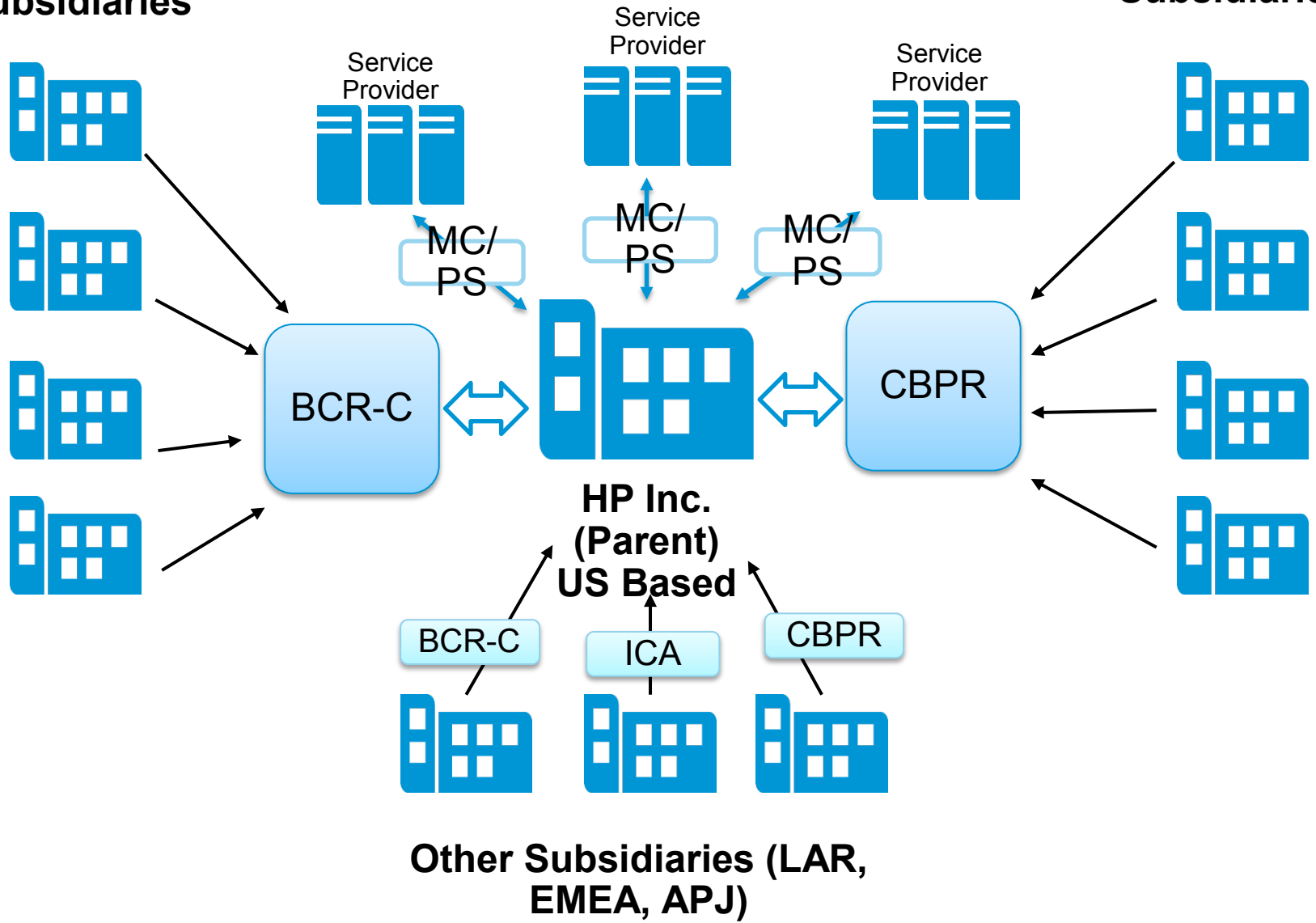
# Global Interoperability of Privacy Frameworks



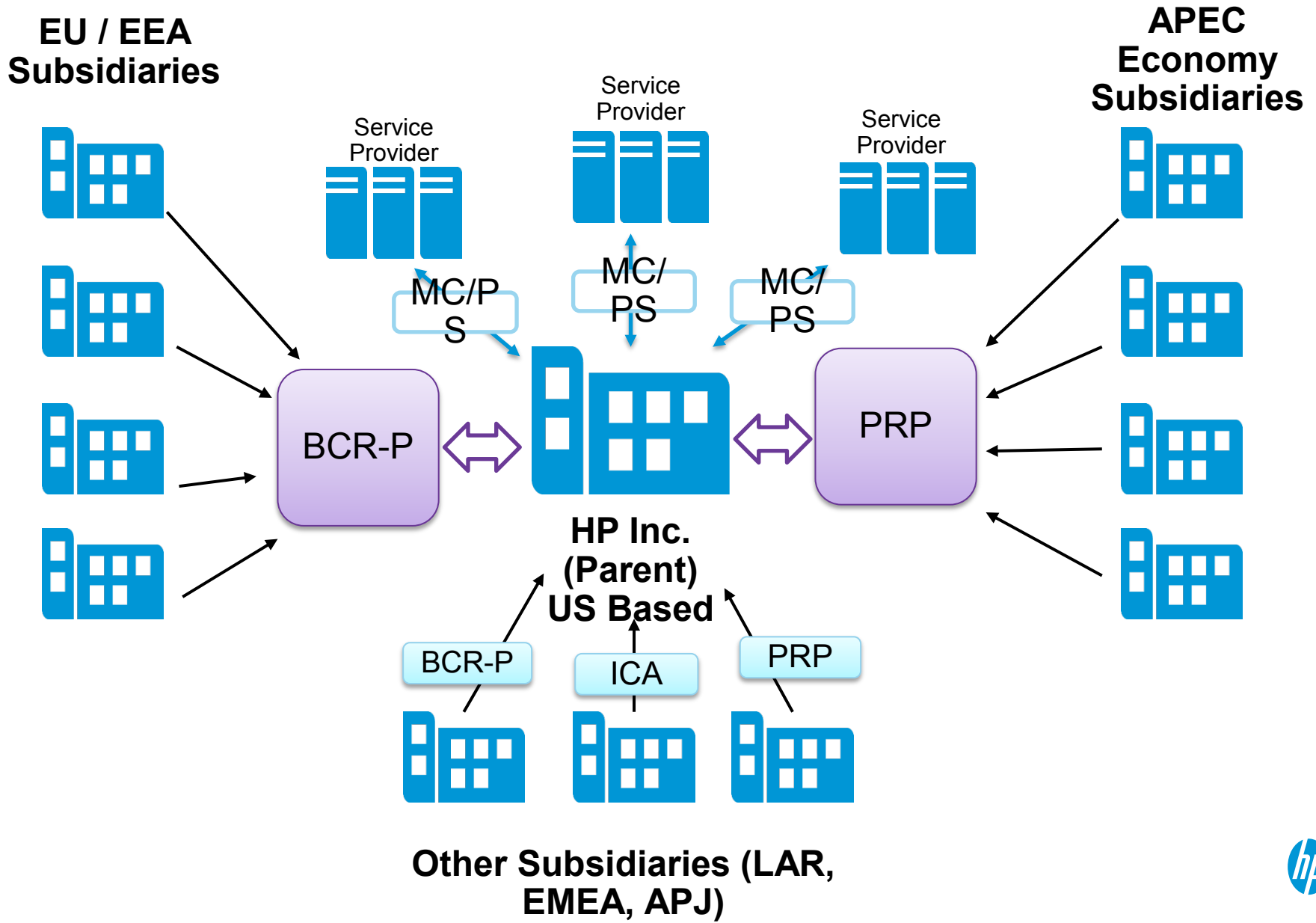
# Certifications as Interoperability - HP as Controller

**EU / EEA  
Subsidiaries**

**APEC Economy  
Subsidiaries**



# Certifications as Interoperability - HP as Controller





An aerial photograph of a kitesurfer riding a wave on a vibrant blue ocean. The kitesurfer is positioned in the lower-left quadrant, leaving a white wake. A colorful kite with yellow, green, and red panels is visible in the upper-right quadrant. The text "THANK YOU" is overlaid in the middle-left area.

# THANK YOU

@jesquenaziMX





## **Session III**

# **A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join**

**Harvey Jang**

Director, Global Privacy & Data Protection, Cisco

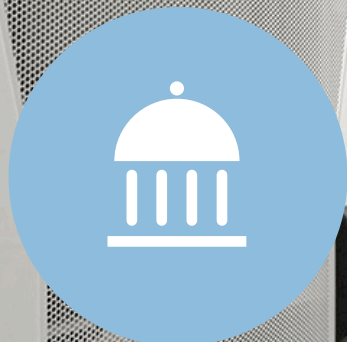


**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

# Strategic Considerations



Legal  
Obligations



Risk Landscape



Customer &  
Market Expectations



Competitive  
Differentiation



Asia-Pacific  
Economic Cooperation



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP



# Data Protection Program



Policies and  
Standards



Identification and  
Classification



Data Risk and  
Organizational Maturity



Incident  
Response



Oversight and  
Enforcement



Privacy by Design &  
Privacy Impact Assessments



Security by Design &  
Data Loss Prevention



Awareness and  
Education

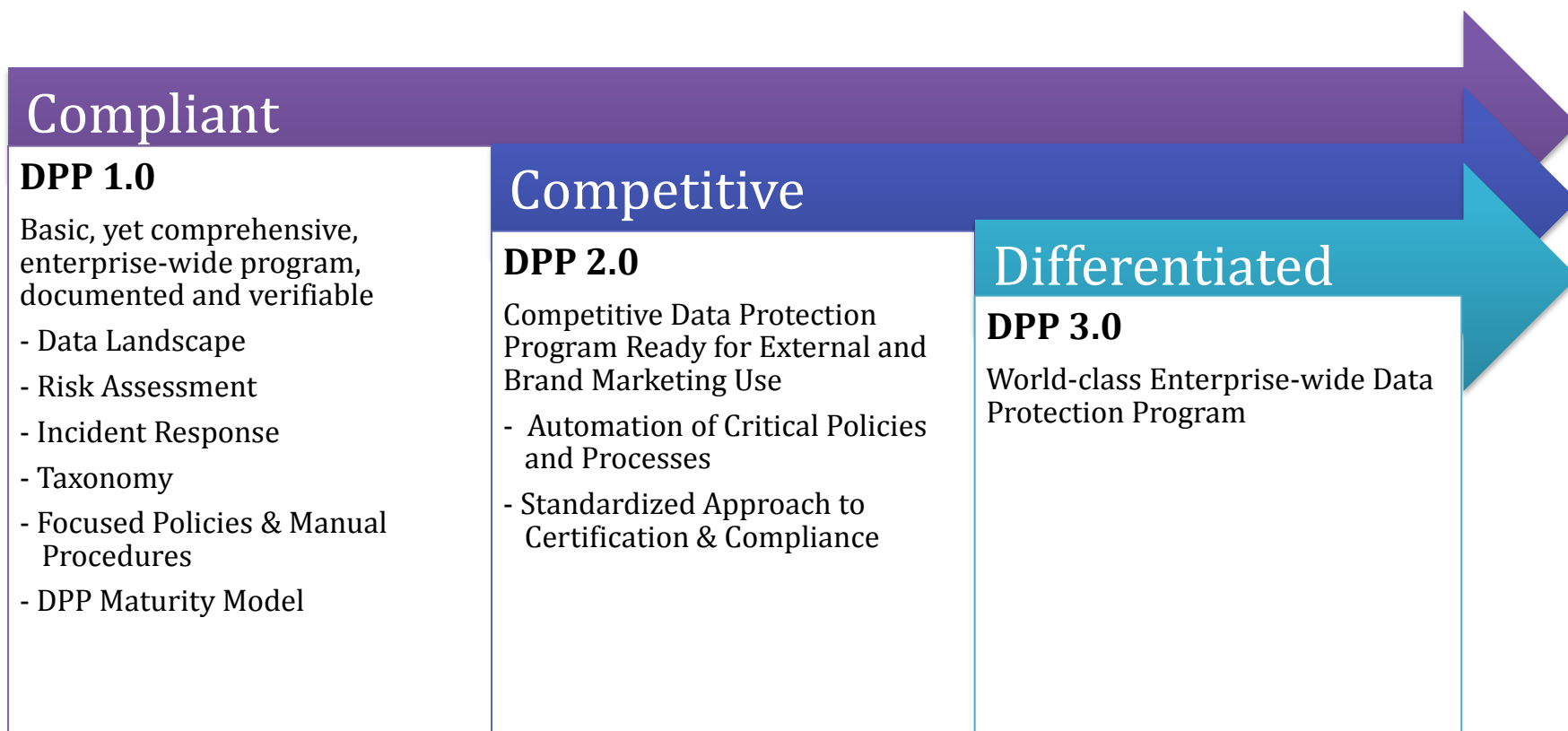


Asia-Pacific  
Economic Cooperation



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

# Data Protection Journey



## CBPR Benefits

- Demonstrate Compliance & Accountability
- External Validation/Testing
- Global Interoperability and Consistency
- Meet Employee and Customer Expectations
- Build and Enhance Trust



## **Session III**

# **A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join**

**Huey Tan**

Senior Privacy Counsel, Apple



**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

## Session III

# A Deep-Dive Into the Benefits of the CBPR – Why Companies Should Join

**Moderator:** Markus Heyder, Vice President and Senior Policy Counselor, CIPL

- ❖ Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.
- ❖ Harvey Jang, Director, Global Privacy & Data Protection, Cisco
- ❖ Annelies Moens, Deputy Managing Director, Information Integrity Solutions
- ❖ Daisuke Nagasaki, Deputy Director, International Affairs Office, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan (METI)
- ❖ Huey Tan, Senior Privacy Counsel, Apple



# Break



**Asia-Pacific  
Economic Cooperation**



## Session IV

### A Deep-Dive into the Certification Process

**Moderator:** Markus Heyder, Vice President and Senior Policy Counselor, CIPL

- ❖ Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.
- ❖ Josh Harris, Director of Policy, TRUSTe
- ❖ Hiromu Yamada, Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- ❖ Hilary Wandall, AVP, Compliance and CPO, Merck & Co., Inc.





## **ENABLING LEGAL COMPLIANCE & CROSS-BORDER DATA TRANSFERS WITH THE APEC CROSS-BORDER PRIVACY RULES**

**Session IV: A Deep-Dive into the Certification  
Process**

**Powering Privacy Compliance and Trust**



# Organizational Review Process

Category/Section	Description	Assigned to	No. of Questions
PSM Scoping	The following questions are part of the PSM's initial investigation and scoping review. Please review for accuracy.	Default	23
Introductory Questions		Default	9
Notice	<p>The questions in this section are directed towards:</p> <p>(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may be used; AND</p> <p>(b) ensuring that, subject to the qualifications listed in part II, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.</p>	Default	10
Collection Limitation	The questions in this section are directed towards ensuring that collection of information is limited to the stated purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.	Default	3
Uses of Personal Information	The questions in this section are directed toward ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization.	Default	4

# Example of Initial Attestation Form

## and Correction

Question	Answer Type
Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual?	YES_NO
Upon request, do you provide individuals access to the personal information that you hold about them?	YES_NO
Do you provide access within a reasonable timeframe following an individual's request for access?	YES_NO
Is information communicated in a reasonable manner that is generally understandable (in a legible format)?	YES_NO
Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?	YES_NO
Do you charge a fee for providing access?	YES_NO
Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted?	YES_NO

re

Publish Assessment

◀ Security Safeguards

Accountab

# Remediation Process



## TRUSTe Privacy Findings Report

6

### b. Required Changes

The following changes are required to complete certification and to display the TRUSTe seal.

<b>Review Findings #1:</b>	
<b>Finding:</b>	
<b>Required Change:</b>	
<b>Resolution:</b> <u>Pending</u> /Yes	<b>Date Resolved:</b>
	<b>Resolved by:</b>
<b>Review Findings #2:</b>	
<b>Finding:</b>	
<b>Required Change:</b>	
<b>Resolution:</b> <u>Pending</u> /Yes	<b>Date Resolved:</b>
	<b>Resolved by:</b>
<b>Review Findings #3:</b>	
<b>Finding:</b>	



**Josh Harris**

[jharris@truste.com](mailto:jharris@truste.com)

**Powering Privacy Compliance and Trust**

## **Session IV**

# **A Deep-Dive into the Certification Process**

**Hiromu Yamada**

Japan Institute for Promotion of Digital Economy and Community (JIPDEC)



**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

# JIPDEC: Accountability Agent in Japan



## JIPDEC's objective

Our objective is to establish a safe and secure digital society.

Through the actions of our daily routines, such as driving a car, visiting a doctor, or making online purchases, multitudes of content-rich data are produced. Being able to refine and use this data holds great promise not only for us as the creators of the data but also for others, by way of monetized anonymous data streams. Yet if there is no mechanism for the correct and responsible use of this data, it will be impossible to establish a safe and secure digital society. It is these requirements that JIPDEC is addressing, with the operation of the PrivacyMark System, Information Security Management System (ISMS) and other projects and research topics, to form the foundation of a safe and secure digital society.

## TOP

■ Accredited Personal  
Information Protection  
Organizations

Executive Perspective

About us

Our Activities

Access

<http://english.jipdec.or.jp/index.html>



- Becomes Target Entities of Accredited Personal Information Protection Organizations of JIPDEC which is AA.
- Flow from application to registration
  - The procedure includes **1. Application, 2. Review (documentation and on-site), 3. Board of review, 4. Registration.**

procedure	Main documents submitted by Applicant	What Accredited Personal Information Protection Organizations do
application	1. Intake Questionnaire 2. Application form	1. Confirm documents 2. Check about the compliance with CBPR regulations 3. Charge the review fee 4. Accept application form
Review (documentation)	1. Regulations (Japanese/English) 2. Publicized documents (Japanese/English) 3. Internal regulations, etc. needed to review (Japanese)	1. Hearing (Interviews overall handling about personal information) 2. Documentation review
Review (on-site)	(Attendance and Explanation)	1. Check the operation situation of applicant on-site (Check mainly security, etc.)
Board of review		1. Hold Board of review and determine the certification 2. Charge the management fee of the certification
registration		1. Confirm the payment of the management fee of the certification 2. Issue the certificate 3. Registration of organization name/Publication of the name on web site.

- Intake Questionnaire is intended to describe the applicant's answers to 50 questions about the handling of personal information, **in accordance with the APEC principles.**

(Supporting documents, etc. are also needed)

- The contents of the questions are coordinated with domestic laws in government.
  - The System does not certify the compliance with domestic laws, but, the idea is that there will be no violation of laws about handling personal information, as a result, if business entities follow the scheme.

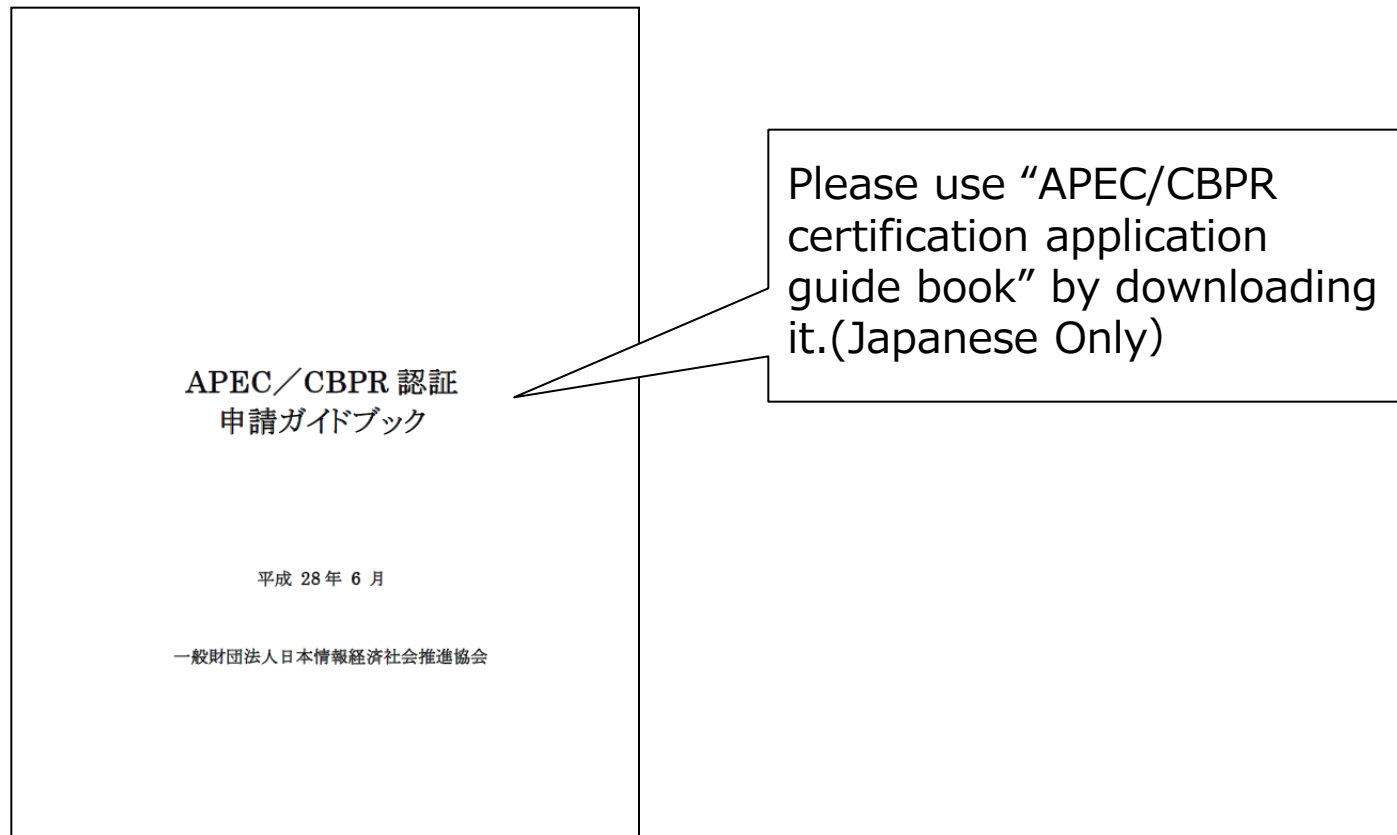
 Asia-Pacific Economic Cooperation	
 2016.06	
APEC 越境プライバシールールシステム 事前質問書	
基本情報.....	2
通知.....	5
通知に関する規定の条件.....	7
取得の制限.....	8
個人情報の利用.....	9
選択.....	11
選択手順に関する規定の条件.....	13
個人情報の完全性.....	14
セキュリティ対策.....	15
アクセス及び訂正.....	18
アクセス及び訂正手順に関する規定の条件.....	18
責任.....	22
一般.....	22
個人情報が移転された場合の責任の維持.....	23

Page | 1



■ **We will conduct an individual consultation to business entities which is considering applying for CBPR certification.**

- E-mail [nintei-inq@tower.jipdec.or.jp](mailto:nintei-inq@tower.jipdec.or.jp)
- Web [http://www.jipdec.or.jp/protection\\_org/index.html](http://www.jipdec.or.jp/protection_org/index.html)



## **Session IV**

# **A Deep-Dive into the Certification Process**

**Hilary Wandall**

AVP, Compliance and CPO, Merck & Co., Inc.

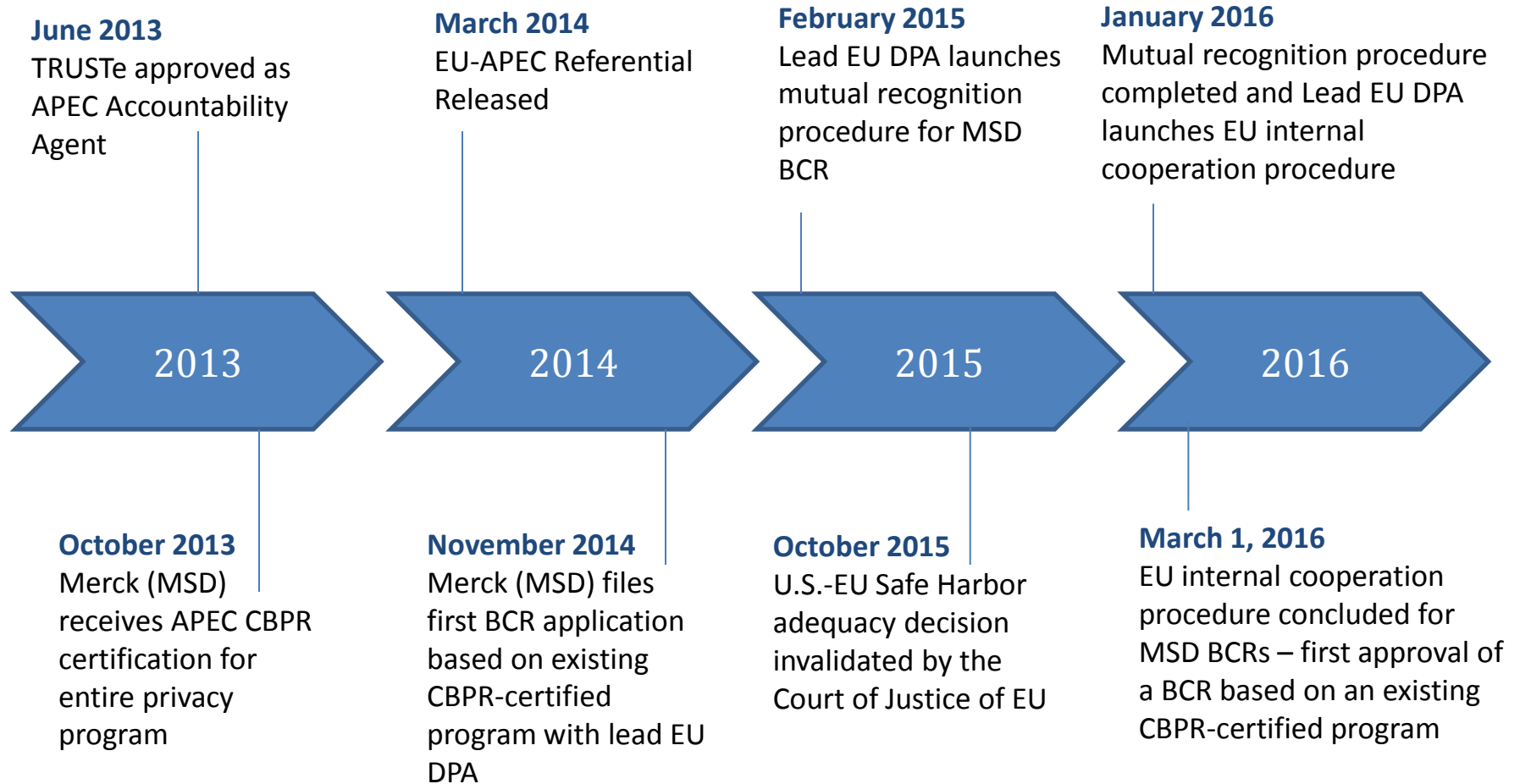


**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

# MSD Journey to CBPR-BCR Interoperability in Practice



## **Session IV**

# **A Deep-Dive into the Certification Process**

**Jacobo Esquenazi**

Global Privacy Strategist, HP, Inc.



**Asia-Pacific  
Economic Cooperation**



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

## Session IV

### A Deep-Dive into the Certification Process

**Moderator:** Markus Heyder, Vice President and Senior Policy Counselor, CIPL

- ❖ Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.
- ❖ Josh Harris, Director of Policy, TRUSTe
- ❖ Hiromu Yamada, Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- ❖ Hilary Wandall, AVP, Compliance and CPO, Merck & Co., Inc.



## Session V

### Enforcing the CBPR

**Moderator:** Bojana Bellamy, President, CIPL

- ❖ Melinda Claybaugh, Counsel for International Consumer Protection, Office of International Affairs, US Federal Trade Commission
- ❖ Andrew Flavin, Policy Advisor, Office of Digital Services Industries, International Trade Administration, US Department of Commerce



# THANK YOU!

Please return name badges.

Visit our website at  
[www.informationpolicycentre.com](http://www.informationpolicycentre.com)



Asia-Pacific  
Economic Cooperation



Centre for  
Information  
Policy  
Leadership  
Hunton & Williams LLP

**Appendix 5**  
**Information Integrity Solutions Report for APEC**  
*Preliminary assessment: Potential benefits for*  
*APEC economies and businesses joining the CBPR System*





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

Report for APEC

February 2016

INFORMATION  
INTEGRITY  
SOLUTIONS

managing the **privacy** of **individuals**  
is **complex** and we can help you get  
it **right**

# Table of Contents

<b>1. APEC and Privacy .....</b>	<b>4</b>
1.1 Objective .....	4
1.1.1 Scope of report.....	4
1.1.2 Context .....	5
1.1.3 Summary of overall assessment .....	6
<b>2. Government Stakeholders .....</b>	<b>6</b>
2.1 Trade benefits .....	6
2.1.1 Advancement towards global trade and economic growth policy objectives .....	6
2.1.2 International cooperation.....	7
2.1.3 Increased confidence .....	8
2.1.4 Procurement processes .....	8
2.2 External stakeholder benefits.....	8
2.2.1 Tool to maintain free flow of data with privacy protection .....	8
2.2.2 Maintain trust in APEC economies.....	9
2.2.3 Assurance .....	9
<b>3. Business Stakeholders .....</b>	<b>9</b>
3.1 Trade benefits .....	10
3.1.1 Appropriate privacy protection .....	10
3.1.2 Interoperability.....	11
3.1.3 Foreign direct investment.....	12
3.2 Internal organisational benefits .....	12
3.2.1 Future proofing for change .....	12
3.2.2 One global compliance system .....	12
3.2.3 Efficiency .....	13
3.2.4 Flexibility.....	13
3.2.5 Regulatory treatment.....	14
3.3 External stakeholder benefits.....	14
3.3.1 Assurance .....	14
3.3.2 Communication with consumers .....	15
3.3.3 Trust .....	15
3.3.4 Good faith and public relations.....	15
<b>4. Regulator Stakeholders .....</b>	<b>15</b>
4.1 Internal regulatory benefits.....	16
4.1.1 Role of accountability agents and their overseers .....	16
4.1.2 Improved strategic resource allocation .....	17

4.2	External regulatory benefits .....	17
4.2.1	Assurance .....	17
4.2.2	Choice .....	18
4.2.3	Raises the benchmark.....	18
5.	<b>Overall Assessment .....</b>	<b>18</b>
6.	<b>References.....</b>	<b>20</b>
7.	<b>Appendix 1 – Economy Overviews .....</b>	<b>22</b>
7.1	Japan.....	22
7.2	Singapore .....	23
7.3	USA .....	24
7.4	Canada.....	25
7.5	Mexico .....	26
8.	<b>Appendix 2 – Stakeholders Consulted.....</b>	<b>27</b>
8.1	Government.....	27
8.2	Business .....	28
8.3	Regulator .....	31
9.	<b>Appendix 3 – About the Authors .....</b>	<b>32</b>

# 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).<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup>

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.<sup>4</sup> 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](http://www.apec.org)) and at the CBPR dedicated website ([www.cbprs.org](http://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),<sup>5</sup> 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.<sup>6</sup> 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”.<sup>7</sup>

### 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.<sup>8</sup>

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.<sup>9</sup>

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:<sup>10</sup>

- Company based in Economy A
- With operations in Economy B
- Capturing data on citizens in Economies A, B, C, and D
- Leverages a cloud service provider based in Economy E
- Cloud service provider replicates data across facilities in Economies 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”.<sup>11</sup>

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.

Viet Nam 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, Viet Nam 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".<sup>12</sup>

#### 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.<sup>13</sup>

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 Viet Nam 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.<sup>14</sup>

These improved facilities for Viet Nam 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.<sup>15</sup>

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.<sup>16</sup>

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.<sup>17</sup>

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.<sup>18</sup>



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

- <sup>1</sup> See APEC, *APEC Cross-Border Privacy Rules System* <<http://www.apec.org/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf>>.
- <sup>2</sup> 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](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](http://www.apec.org/~media/Files/Groups/ECSG/CBPR/20140430_CBPR_Japan_Final_Report.pdf)>.
- <sup>3</sup> TRUSTe, 'TRUSTe Certified Companies' <<https://www.truste.com/consumer-resources/trusted-directory/>>.
- <sup>4</sup> APEC, '2015 APEC economic leaders' week opens in Manila' (13 November 2015) <[http://www.apec.org/Press/News-Releases/2015/1113\\_CSOM.aspx](http://www.apec.org/Press/News-Releases/2015/1113_CSOM.aspx)>.
- <sup>5</sup> APEC, *Privacy Recognition for Processors: Purpose and Background* (February 2015) <<https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf>>.
- <sup>6</sup> APEC, 'About APEC: History' <<http://www.apec.org/About-Us/About-APEC/History.aspx>>.
- <sup>7</sup> Trans-Pacific Partnership Agreement, 'Chapter 14: Electronic Commerce' <<http://dfat.gov.au/trade/agreements/tpp/official-documents/Documents/14-electronic-commerce.pdf>>.
- <sup>8</sup> 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](http://www.apec.org/~media/files/groups/ecsg/20140307_referential-bcr-cbpr-reqs.pdf)>.
- <sup>9</sup> 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>>.
- <sup>10</sup> 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](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\\_b\\_order\\_data\\_flows.pdf](http://www.iispartners.com/downloads/IIS_Success_through_stewardship_Best_practice_in_cross_b_order_data_flows.pdf)>, p. 20.

<sup>11</sup> 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](http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf)>, p. 13.

<sup>12</sup> 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](http://mddb.apec.org/Documents/2012/ECSG/DSP1/12_ecsg_dps1_007.pdf)>, p. 4.

<sup>13</sup> 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>>.

<sup>14</sup> Dang Cong San, 'Viet Nam'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>>.

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

<sup>16</sup> APEC, 'Ongoing APEC CBPR requirements for Accountability Agents'

<<http://www.cbprs.org/Agents/OngoingRequirements.aspx>>.

<sup>17</sup> 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>>.

<sup>18</sup> 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-](https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its)

[releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its](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 economy. 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 an economy 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

## Appendix 2 – Stakeholders Consulted

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 Accenture DBS Bank Deutsche Bank General Electric International SOS Mastercard OCBC Standard Chartered UBS 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, Viet Nam 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](mailto:inquiries@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN107 611 898

Produced By

Markus Heyder [mheyder@hunton.com](mailto:mheyder@hunton.com)  
Centre for Information Policy Leadership at Hunton & Williams LLP  
2200 Pennsylvania Avenue, NW  
Washington, DC 20037  
Tel: 202-955-1563  
Email: [information@hunton.com](mailto:information@hunton.com)  
Website: [www.hunton.com](http://www.hunton.com) or [www.informationpolicycentre.com](http://www.informationpolicycentre.com)

For  
Asia Pacific Economic Cooperation Secretariat  
35 Heng Mui Keng Terrace  
Singapore 119616  
Tel: (65) 68919 600  
Fax: (65) 68919 690  
Email: [info@apec.org](mailto:info@apec.org)  
Website: [www.apec.org](http://www.apec.org)

© 2016 APEC Secretariat