THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 3

APEC OVERVIEW

Ellyce R Cooper and Alan Charles Raul[1]

I OVERVIEW

The Asia-Pacific Economic Cooperation (APEC) is an organisation of economic entities in the Asia-Pacific region formed to enhance economic growth and prosperity in the region. It was established in 1989 by 12 Asia-Pacific economies as an informal ministerial-level dialogue group. Because APEC is primarily concerned with trade and economic issues, the criterion for membership is being an economic entity rather than a nation. For this reason, its members are usually described as 'APEC member economies' or 'APEC economies'. Since 1993, the heads of the member economies have met annually at an APEC Economic Leaders Meeting, which has since grown to include 21 member economies as of July 2018: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States and Vietnam.[2] Collectively, the 21 member economies account for more than half of world real GDP in purchasing power parity and over 44 per cent of total world trade.[3]

The main aim of APEC is to fulfil the goals established in 1994 at the Economic Leaders Meeting in Bogor, Indonesia of free and open trade and investment in the Asia-Pacific area for both industrialised and developing economies. APEC established a framework of key areas of cooperation to facilitate achievement of these 'Bogor Goals'. These areas, also known as the three pillars of APEC, are the liberalisation of trade and investment, business facilitation and economic and technical cooperation. In recognition of the exponential growth and transformative nature of electronic commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work towards the development of consistent legal, regulatory and policy

1 Ellyce R Cooper and Alan Charles Raul are partners at Sidley Austin LLP. The current authors wish to thank Catherine Valerio Barrad, who was the lead author for the original version of this chapter and made substantial contributions to prior updates. She was formerly a partner at Sidley and is now university counsel for San Diego State University. Sheri Porath Rockwell, an associate at Sidley Austin LLP, assisted in preparing this chapter.

2 The current list of APEC member economies can be found at www.apec.org/About-Us/About-APEC/Member-Economies.aspx.

3 See www.apec.org/FAQ.

environments in the Asia-Pacific area.[4] It further established the Data Privacy Subgroup under the ECSG in 2003 to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.[5]

Because of varied domestic privacy laws among the member economies (including economies at different stages of legislative recognition of privacy), APEC concluded that a regional agreement that creates a minimum privacy standard would be the optimal mechanism for facilitating the free flow of data among the member economies (and thus promoting electronic commerce). The result was the principles-based APEC Privacy Framework, which was endorsed by the APEC economies in 2005. Although consistent with the original Organisation for Economic Co-operation and Development (OECD) Guidelines, the APEC Privacy Framework also provided assistance to member economies in developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows.

Unlike other privacy frameworks, APEC does not impose treaty obligation requirements on its member economies. Instead, the cooperative process among APEC economies relies on non-binding commitments, open dialogue and consensus. Member economies undertake commitments on a voluntary basis. Consistent with this approach, the APEC Privacy Framework is advisory only and thus has few legal requirements or constraints.

In 2011, APEC implemented the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC is also working with the EU to study the potential interoperability of the APEC and the EU's new General Data Protection Regulation (GDPR), building upon the issuance in 2014 of a joint referential document mapping requirements of APEC and the EU's former data protection regime.

The APEC Privacy Framework, the CBPR and PRP systems, the cooperative privacy enforcement system and APEC–EU collaborative efforts are all described in more detail below.

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework, endorsed by APEC in 2005, was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow of information in support of economic development. It was an outgrowth of the 1998 APEC Blueprint for Action on Electronic Commerce, which recognised that the APEC member economies needed to develop and implement legal and

4 The ECSG was originally established as an APEC senior officials' special task force, but in 2007 was realigned to the Committee on Trade and Investment. This realignment underscores the focus within the ECSG, and its Data Privacy Subgroup, on trade and investment issues.

5 APEC endorsed the Blueprint in 1998 to 'develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy'. See APEC Privacy Framework (2005), Paragraph 1 (available at www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx).

regulatory structures to build public confidence in the safety and security of electronic data flows (including consumers' personal data) to realise the potential of electronic commerce. This recognition was the impetus behind the development of the Privacy Framework. Thus, the APEC objective of protecting informational privacy arises in the context of promoting trade and investment, rather than primarily to protect basic human rights as in the European Union.

The APEC Privacy Framework represents a consensus among economies with different legal systems, cultures and values, and that at the time of endorsement were at different stages of adoption of domestic privacy laws and regulations. Thus, the Framework provided a basis for the APEC member economies to acknowledge and implement basic principles of privacy protection, while still permitting variation among them. It further provides a common basis on which to address privacy issues in the context of economic growth and development, both among the member economies and between them and other trading entities. The Privacy Framework was updated in 2015 to account for the development of new technologies and developments in the marketplace and to ensure that the free flow of information and data across borders is balanced with effective data protections.[6] While updates were made to the preamble and commentary sections, the basic principles of the Framework remained unchanged. Further updates to the Privacy Framework are in the planning stages.[7]

ii The Privacy Framework

The Privacy Framework has four parts:

a Part I is a preamble that sets out the objectives of the principles-based Privacy Framework and discusses the basis on which consensus was reached;

b Part II describes the scope of the Privacy Framework and the extent of its coverage;

c Part III sets out the information privacy principles, including an explanatory commentary on them; and

d Part IV discusses the implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and scope of the Privacy Framework (Parts I and II)

The market-oriented approach to data protection is reflected in the objectives of the Privacy Framework, which include – in addition to the protection of information – the prevention of unnecessary barriers to information flows, the promotion of uniform approaches by multinational businesses to the collection and use of data, and the facilitation of domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework was designed for broad-based acceptance across member economies by encouraging compatibility while still respecting the different cultural, social and economic requirements within the economies. As such, it sets an advisory minimum standard and permits member economies to adopt stronger, country-specific data protection laws.

The Privacy Framework cautions that the principles should be interpreted as a whole, rather than individually, because they are interconnected, particularly in how they balance privacy rights and the market-oriented public interest. These principles are not intended to

6 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx.

7 https://www.apec2018png.org/media/press-releases/revise-framework-conducive-for-e-commerce-environment.

impede governmental activities within the member economies that are authorised by law, and thus the principles allow exceptions that will be consistent with particular domestic circumstances.[8] The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.[9]

The nine principles of the Privacy Framework (Part III)

Given that seven of the original APEC member economies were members of the OECD, it is not surprising that the original APEC Privacy Framework was based on the original OECD Guidelines. Similarly, the 2015 update was based on a 2013 update to the OECD's Guidelines.[10] The APEC privacy principles address personal information about living individuals and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.

While based on the OECD Guidelines, the APEC principles are not identical to them. Missing are the OECD Guidelines of 'purpose specification' and 'openness', although aspects of these can be found within the nine principles – for example, purpose limitations are incorporated in Principle IV regarding use of information. The APEC principles also permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines on notice. In general, the APEC principles reflect the objective of promoting economic development and the respect for differing legal and social values among the member economies.

Principle I – preventing harm

This principle provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information and that remedies for infringement be proportionate to the likelihood and severity of harm.

Principle II – notice

The notice principle addresses the information that a data controller must include in a notice to individuals when collecting their personal information. It also requires that all reasonable steps be taken to provide the notice either before or at the time of collection and if not, then as soon after collection as is reasonably practicable. The principle further provides for an exception for notice of collection and use of publicly available information.

Principle III – collection limitation

This principle provides for the lawful and fair collection of personal information limited to that which is relevant to the purpose of collection and, where appropriate, with notice to, or consent of, the data subject.

8 See APEC Privacy Framework (2015), Paragraph 18.

9 See APEC Privacy Framework (2015), Paragraph 17.

10 See APEC Privacy Framework (2015), Paragraph 5.

Principle IV – uses of personal information

This principle limits the use of personal information to those uses that fulfil the purpose of collection and other compatible or related purposes. It includes exceptions for information collected with the consent of the data subject and collection necessary to complete a request of the data subject or as required by law.

Principle V – choice

The choice principle directs that, where appropriate, individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information, with an exception for publicly available information. This principle also contemplates that, in some instances, consent can be implied or is not necessary.

Principle VI – integrity of personal information

This principle states that personal information should be accurate, complete and kept up to date to the extent necessary for the purpose of use.

Principle VII – security safeguards

This principle requires that security safeguards be applied to personal data that are appropriate and proportional to the likelihood and severity of threatened harm, the sensitivity of the data and the context in which it is held, and that the safeguards be periodically reassessed.

Principle VIII – access and correction

The access and correction principle directs that individuals have the right of access to their personal information within a reasonable time and in a reasonable manner, and may challenge its accuracy and request appropriate correction. This principle includes exceptions when the burden of access or correction outweighs the risks to individual privacy, the information is subject to legal or security holds, or where privacy rights of other data subjects may be affected.

Principle IX – accountability

This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles and that, when transferring personal information, it should take reasonable steps to ensure that the recipients also protect the information in a manner that is consistent with the principles. This has often been described as the most important innovation in the APEC Privacy Framework and it has been influential in encouraging other privacy regulators to consider similar accountability processes tailored to the risks associated with that specific data.

Unlike other international frameworks, the APEC Privacy Framework neither restricts the transfer of data to countries without APEC-compliant data protection laws nor requires such a transfer to countries with APEC-compliant laws. Instead, APEC adopted the accountability principle in lieu of data import and export limitations as being more consistent with modern business practices and the stated objectives of the Privacy Framework.

Implementation (Part IV)

Because APEC is a cooperative organisation, the member economies are not required to convert the Privacy Framework into domestic legislation. Rather, the Privacy Framework encourages

the member economies to implement it without requiring or proposing any particular means of doing so. It suggests that there are 'several options for giving effect to the Framework [. . .] including legislative, administrative, industry self-regulatory or a combination of these policy instruments'.[11] The Framework advocates 'having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from [] violations' and supports a choice of remedies appropriate to each member economy.[12] The Privacy Framework does not contemplate a central enforcement entity.

Thus, the APEC Privacy Framework contemplates variances in implementation across member economies. It encourages member economies to share information, surveys and research and to expand their use of cooperative arrangements (such as the Cross-Border Privacy Enforcement Arrangement (CPEA (see Section III.iii)) to facilitate cross-border cooperation in investigation and enforcement.[13]

iii Data privacy individual action plans (IAPs)

Data privacy IAPs are periodic, national reports to APEC on each member economy's progress in adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.[14] The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2018, 14 member economies have IAPs.[15]

III APEC CROSS-BORDER DATA TRANSFER

i Data Privacy Pathfinder initiative

When originally enacted in 2005, the APEC Privacy Framework did not explicitly address the issue of cross-border data transfer, but rather called for cooperative development of cross-border privacy rules.[16] In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder initiative with the goal of achieving accountable cross-border flows of personal information within the Asia-Pacific region. The Data Privacy Pathfinder initiative contains general commitments leading to the development of an APEC CBPR system that would support accountable cross-border data flows consistent with the APEC Privacy Principles.

The main objectives of the Pathfinder initiative are to promote a conceptual framework of principles for the execution of cross-border privacy rules across APEC economies, to develop consultative processes among the stakeholders in APEC member economies for the development of implementing procedures and documents supporting cross-border privacy rules and to implement an accountable cross-border privacy system. Both the CBPR system and the CPEA – cross-border privacy systems that facilitate data protection and privacy enforcement – are outcomes of the Pathfinder initiative.[17]

11 See APEC Privacy Framework (2015), Paragraph 37.

12 See APEC Privacy Framework (2015), Paragraphs 53, 37.

13 See APEC Privacy Framework (2015), Paragraphs 57–64.

14 See APEC Privacy Framework (2015), Paragraph 55.

15 See https://www.apec.org/Groups/Committeee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

16 See APEC Privacy Framework (2005), Paragraphs 46–48.

17 See Sctions III.ii and III.iii

ii The CBPR system

The APEC CBPR system, endorsed in 2011, is a voluntary accountability-based system governing electronic flows of private data among APEC economies. As of July 2018, six APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea, Singapore (a recent addition) and the United States – with more expected to join.[18]

In general, the CBPR system requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards that meet or exceed the APEC Privacy Framework. The system is designed to build consumer, business and regulator trust in the cross-border flow of electronic personal data in the Asia-Pacific region. One of the goals of the CBPR system is to 'lift the overall standard of privacy protection throughout the [Asia-Pacific] region' through voluntary, enforceable standards set out within it.[19]

Organisations that choose to participate in the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognised accountability agent to assess compliance with the programme. Upon certification, the practices and policies will become binding on that organisation and enforceable through the relevant privacy enforcement authority.[20]

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is composed of nominated representatives of participating economies and any working groups the Panel establishes. The Joint Oversight Panel operates according to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.[21]

Accountability agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private accountability agents) or under applicable domestic laws and regulations (accountability agents and privacy enforcement authorities).

The CBPR system has its own website, which includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports and template forms.[22]

Participation in the CBPR system

Only APEC member economies may participate in the CBPR system and must meet three requirements:

a participation in the APEC CPEA with at least one privacy enforcement authority;

18 https://www.huntonprivacyblog.com/2018/03/08/singapore-joins-the-apec-cbpr-and-prp-systems/#more-14134 (Australia, the Philippines and Chinese Taipei are actively working to join CBPR and PRP systems).

19 See www.cbprs.org/Government/GovernmentDetails.aspx.

20 A privacy enforcement authority is 'any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings'. 'Privacy Law' is further defined as 'laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework'. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, at 10.

21 See cbprs.blob.core.windows.net/files/JOP%20Charter.pdf; and cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf.

22 See www.cbprs.org/default.aspx.

b submission of a letter of intent to participate addressed to the chairs of the APEC ECSG, the Data Privacy Subgroup and the CBPR system Joint Oversight Panel providing:
- confirmation of CPEA participation;
- identification of the APEC CBPR system-recognised accountability agent that the economy intends to use;
- details regarding relevant domestic laws and regulations, enforcement entities and enforcement procedures; and

c submission of the APEC CBPR system programme requirements enforcement map.

The Joint Oversight Panel of the CBPR issues a findings report that addresses whether the economy has met the requirements for becoming an APEC CBPR system participant. An applicant economy becomes a participant upon the date of a positive findings report.

Accountability agents

The APEC CBPR system uses APEC-recognised accountability agents to review and certify participating organisations' privacy policies and practices as compliant with the APEC CBPR system requirements, including the APEC Privacy Framework. Applicant organisations may participate in the CBPR system only upon this certification and it is the responsibility of the relevant accountability agent to undertake certification of an applicant organisation's compliance with the programme requirements. An accountability agent makes no determination as part of the CBPR verification programme regarding whether the applicant organisation complies with domestic legal obligations that may differ from the CBPR system requirements.

APEC CBPR system requirements for accountability agents[23] include:

a being subject to the jurisdiction of a privacy enforcement authority in an APEC economy participating in the CBPR system;

b satisfying the accountability agent recognition criteria;[24]

c agreeing to use the CBPR intake questionnaire to evaluate applicant organisations (or otherwise demonstrate that propriety procedures meet the baseline requirements of the CBPR system); and

d completing and signing the signature and contact information form.[25]

Proposed accountability agents are nominated by an APEC member economy and, following an application and review process by the Joint Oversight Panel, may be approved by the ECSG upon recommendation by the Panel. Any APEC member economy may review the recommendation as to any proposed accountability agent and present objections to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed 'recognised'. Complaints about a recognised accountability agent are reviewed by the Joint Oversight Panel, which has the discretion to request investigative or enforcement assistance from the relevant privacy enforcement authority in the APEC economy where the agent is located.

No accountability agent may have an actual or potential conflict of interest, nor may it provide services to entities it has certified or that have applied for certification. It must

23 http://www.cbprs.org/Agents/CBPRsRequirements.aspx.

24 See cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf.

25 See cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf.

continue to monitor certified organisations for compliance with the APEC CBPR system standards and must obtain annual attestations regarding this compliance. It must publish its certification standards and must promptly report all newly certified entities, as well as any suspended or terminated entities to the relevant privacy enforcement authorities and the CBPR Secretariat.

Accountability agents can be either public or private entities and may also be a privacy enforcement authority. Under certain circumstances, an APEC economy may designate an accountability agent from another economy.

Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities.

If only one accountability agent operates in an APEC economy and it ceases to function as an accountability agent for any reason, then the economy's participation in the CBPR system will be suspended and all certifications issued by that accountability agent for businesses will be terminated until the economy once again fulfils the requirements for participation and the organisations complete another certification process.

The CBPR system website contains a chart of recognised accountability agents, their contact information, date of recognition, approved APEC economies for certification purposes and links to relevant documents and programme requirements.[26]

As of July 2018, the CBPR system recognises two accountability agents: TRUSTe and the Japan Institute for Promotion of Digital Economy and Community. TRUSTe is recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community (now called JIPDEC) is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry of the government of Japan.

CBPR system compliance certification for organisations

Only organisations that are subject to the laws of one or more APEC CBPR system-participating economies are eligible for certification regarding personal information transfers between economies.

An organisation that chooses to participate in the CBPR system initiates the process through submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then undertake an iterative evaluation process to determine whether the organisation meets the baseline standards of the programme. The accountability agent has sole responsibility for these first two phases of the CBPR system accreditation process (self-assessment and compliance review).

Organisations that are found to be in compliance with the programme requirements will be certified as CBPR-compliant and identified on the CBPR website. As of June 2018, more than 22 organisations have been APEC CBPR certified, all of which are in the United States, with more in various stages of review.[27] Certified companies must undergo annual recertification. As more accountability agents are recognised in the economies participating in the CBPR system, the number of certified organisations is expected to grow.

26 See www.cbprs.org/Agents/AgentDetails.aspx.

27 A current list of APEC-certified organisations can be found at https://cbprs.blob.core.windows.net/files/Copy%20of%20APEC%20CBPR%20Compliance%20Directory_June2018%20Update_.xlsx.

Effect of the CBPR on domestic laws and regulations

The CBPR system sets a minimum standard for privacy protection requirements and thus an APEC economy may need to make changes to its domestic laws, regulations and procedures to participate in the programme. With that exception, however, the CBPR system does not otherwise replace or modify any APEC economy's domestic laws and regulations. Indeed, if the APEC economy's domestic legal obligations exceed those of the CBPR system, then those laws will continue to apply to their full extent.

PRP system

Because the CBPR system (and the APEC Framework) applies only to data controllers, who remain responsible for the activities conducted by processors on their behalf, APEC member economies and data controllers encouraged the development of a mechanism to help identify qualified and accountable data processors. This led, in 2015, to the APEC PRP programme, which is a mechanism by which data processors can be certified by an accountability agent.[28] This certification can provide assurances to APEC economies and data controllers regarding the quality and compatibility of the processor's privacy policies and practices. The PRP does not change the allocation of responsibility for the processor's practices to the data controller and there is no requirement that a controller engage a PRP-recognised processor to comply with the Framework's accountability principle.

The Joint Oversight Panel of the CBPR administers the PRP program pursuant to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Joint Oversight Panel with Regard to the Privacy Recognition for Processors System.[29] The rules governing certification and ongoing accountability closely track the CBPR framework, requiring the Joint Oversight Panel to engage in a similar evaluative process (e.g., issuing a findings report) as it does for data controllers pursuant to CBPR rules.[30]

As of July 2018, two APEC countries have joined the PRP system – the United States and Singapore – with more expected to follow.[31]

iii The CPEA

One of the key goals of the Privacy Framework is to facilitate domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework does not establish any central enforcement body, but instead encourages the cooperation of privacy enforcement authorities within the Asia-Pacific region. APEC established the CPEA as a multilateral arrangement to facilitate such interaction. The CPEA became the first mechanism in the Asia-Pacific region to promote cooperative assistance among privacy enforcement authorities.

28 The PRP Purpose and Background Document can be found at cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf; and the intake questionnaire for processors is at cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf.

29 https://cbprs.blob.core.windows.net/files/PRP%20Policies%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf.

30 https://cbprs.blob.core.windows.net/files/JOP%20Protocols%20for%20PRP.PDF

31 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

Among other things, the CPEA promotes voluntary information sharing and enforcement by:

a facilitating information sharing among privacy enforcement authorities within APEC member economies;

b supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals and parallel or joint enforcement actions; and

c encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.

The CPEA was endorsed by the APEC ministers in 2009 and commenced in 2010 with five participating economies: Australia, China, Hong Kong China, New Zealand and the United States. Any privacy enforcement authority from any APEC member economy may participate and each economy may have more than one participating privacy enforcement authority. As of July 2018, CPEA participants included over two dozen Privacy Enforcement Authorities from 10 APEC economies.[32]

Under the CPEA, any privacy enforcement authority may seek assistance from a privacy enforcement authority in another APEC economy by making a request for assistance. The receiving privacy enforcement authority has the discretion to decide whether to provide such assistance.

Participation in the CPEA is a prerequisite to participation by an APEC economy in the CBPR system. As a result, each participating APEC economy must identify an appropriate regulatory authority to serve as the privacy enforcement authority in the CBPR system. That privacy enforcement authority must be ready to review and investigate a CBPR complaint if it cannot be resolved by the certified organisation or the relevant accountability agent, and take whatever enforcement action is necessary and appropriate. As more member economies join the CBPR system, this enforcement responsibility is likely to become more prominent.

IV INTEROPERABILITY

Given the global nature of personal information flows, APEC's Data Privacy Subgroup has been involved in collaborative efforts with other international organisations with the goal of improving trust and confidence in the protection of personal information and, ultimately, to enable the associated benefits of electronic commerce to flourish across the APEC region. While privacy regimes such as the APEC Privacy Framework are drafted at the level of principles, there are often very significant differences in the legal and policy implementation of those principles in different economies around the world. In an effort to bridge those differences and find commonality between the two largest privacy systems, in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In August 2017, the APEC/EU Working Group met to discuss the impact GDPR will have on their undertaking.[33] These discussions followed the working group's 2014 release of a document (the Referential) that mapped the CBPR system requirements and rules under

32 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

33 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

the EU's former data protection regime, the EU Data Protection Directive. The Referential identified common and divergent elements of both systems to help multinational companies develop global privacy compliance procedures that were compliant with both systems. In its August 2017 meeting, the Working Group agreed to work to develop a new joint work plan to update its previous work in light of GDPR, focusing on mechanisms that can be used to facilitate cross-border data flows and data protection enforcement between the APEC region and the EU.

V THE YEAR IN REVIEW AND OUTLOOK

In February 2018, the Singapore government officially joined the United States (2012), Mexico (2013), Japan (2014), Canada (2015), and South Korea (2017) as an approved APEC economy participating in the APEC CBPR system.[34] This system is growing slowly, as some economies are waiting to see interest from business and some businesses are waiting for member economies to join. With all the North American Free Trade Agreement countries participating, the CBPR system has taken an important step towards an international presence, which may encourage more APEC member economies and business organisations to participate. IBM became the first company to be certified under the APEC CBPR system, in August 2013; it has been joined by nearly two dozen others, including companies with significant international presence, such as Apple, HP and Merck. All these companies were certified by TRUSTe, the sole accountability agent at the time.

TRUSTe became the first recognised accountability agent under the CBPR system on 25 June 2013 and that status was renewed unanimously by the 21 APEC member economies in early 2015. In early 2016, the 21 APEC member economies approved JIPDEC as Japan's accountability agent. Mexico and Canada have not yet identified their domestic accountability agents.

Following its first enforcement decision under the CBPR against Very Incognito Technologies Inc in June 2016 for misrepresenting its compliance with the CBPR,[35] the FTC continues to bring enforcement actions under APEC. In 2017, the FTC reached settlements with three additional companies – Sentinel Labs, Inc, SpyChatter, Inc and Vir2us, Inc – in actions where the FTC alleged the companies had misrepresented consumers about their participation in the APEC CBPR system.[36] According to the FTC's allegations, all three companies' privacy policies misrepresented that the companies either 'comply with the APEC CBPR' or 'abide by the APEC CBPR'. To settle, the companies signed consent agreements that prohibit them from making misrepresentations about their participation, membership or certification in any privacy or security programme sponsored by a government or self-regulatory or standard-setting organisation.

These cases followed the FTC's announcement in 2016 that it had sent warning letters to 28 companies who claimed compliance with the CBPR despite failing to meet the CBPR requirements. The FTC has brought actions against other companies for similar

34 https://www.mci.gov.sg/~/media/mcicorp/images/budget%20workplan/cos%202018/factsheets/factsheet%20-%20singapore%20joins%20apec%20cross-border%20privacy%20rules%20and%20privacy%20recognition%20for%20processors%20systems.pdf?la=en.

35 See In re Very Incognito Tech, Inc, FTC, No. 162 3034, final order, 21 June 2016.

36 www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about.

misrepresentations in other trans-border programmes, such as the EU–US Safe Harbor Framework and recently under the Privacy Shield programme.[37] The FTC has reminded companies not to mislead consumers about participation in the new EU–US Privacy Shield programme. These new enforcement decisions indicate that the FTC may play a more active role in the future enforcement of the CBPR.

37 In November 2017, the FTC approved settlements with three companies that deceived consumers by falsely claiming participation in the EU-US Privacy Shield programme, https://www.ftc.gov/news-events/press-releases/2017/11/ftc-gives-final-approval-settlements-companies-falsely-claimed.

Appendix 1

ABOUT THE AUTHORS

ELLYCE R COOPER

Sidley Austin LLP

Ellyce Cooper is a partner in the firm's Century City office and a member of the complex commercial litigation and privacy and cybersecurity practices. Ellyce has extensive experience in handling government enforcement matters and internal investigations as well as complex civil litigation. She assists companies facing significant investigations and assesses issues to determine a strategy going forward. Ellyce's diverse experience includes representing clients in internal investigations and government investigations along with responding to and coordinating crisis situations. Her client list includes notable companies from the healthcare, pharmaceutical, accounting, financial, defence and automotive industries. Ellyce earned her JD from the University of California, Los Angeles School of Law and her BA, *magna cum laude*, from the University of California Berkeley.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Data Security, Privacy & Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

SIDLEY AUSTIN LLP

1999 Avenue of the Stars, 17th floor
Los Angeles
California 90067
United States
Tel: +1 310 595 9500
Fax: +1 310 595 9501
ecooper@sidley.com
sheri.rockwell@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com

www.sidley.com

ISBN 978-1-912228-62-1