The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 2

APEC OVERVIEW

Catherine Valerio Barrad and Alan Charles Raul[1]

I OVERVIEW

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 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 August 2014: 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

1 Catherine Valerio Barrad and Alan Charles Raul are partners at Sidley Austin LLP.

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

3 See http://statistics.apec.org/.

commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work toward the development of consistent legal, regulatory and policy 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 2004. Although consistent with the original 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.

APEC recently developed 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. This system is in the early stages of implementation. APEC is also working with the EU to study potential interoperability of the APEC and EU data privacy regimes, and in 2014 issued a joint referential document that maps the requirements of the two regimes for the benefit of businesses that seek certification or approval under both systems.

The APEC Privacy Framework, the Cross-Border Privacy Rules system, the cooperative privacy enforcement system, and the 'APEC–EU Referential' are all described in more detail below.

---

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 […] and consumer protection'. See APEC Privacy Framework, at 2 (available at www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashxInvestment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx).

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework 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 regulatory structures to build public confidence in the safety and security of electronic data flows (including consumers' personal data) in order 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 for 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.

ii The Privacy Framework

The Privacy Framework has four parts. Part I is a preamble that sets out the objectives of the principles-based framework and discusses the basis on which consensus was reached; Part II describes the scope of the Privacy Framework and the extent of its coverage; Part III sets out the information privacy principles, including an explanatory commentary on them; and Part IV discusses implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and Scope of 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 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, the Framework sets an advisory minimum standard, and permits member economies to adopt stronger, and 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 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.[6] The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.[7]

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 APEC Privacy Framework was based on the original OECD Guidelines. 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. 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 1 – 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 2 – 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 3 – 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.

6 See APEC Privacy Framework, paragraph 13.

7 See APEC Privacy Framework, paragraph 12.

Principle 4 – Use 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, collection necessary to complete a request of the data subject, or as required by law.

Principle 5 – 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 6 – Integrity of personal information
This principle states that personal information should be accurate, complete, and maintained up-to-date to the extent necessary for the purpose of use.

Principle 7 – 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 such safeguards be periodically reassessed.

Principle 8 – 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 9 – 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 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 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 methods'.[8] The Framework advocates 'an appropriate array of remedies […] commensurate with the extent of the actual or potential harm' and supports a choice of remedies appropriate to each member economy. 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 engage in cross-border cooperation in investigation and enforcement.[9] This concept later developed into the Cross-Border Privacy Enforcement Arrangement (CPEA – see Section III.iii, *infra*).

iii Data privacy individual action plans

Data privacy individual action plans (IAPs) are periodic, national reports to APEC on each member economy's progress of adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.[10] The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2014, 14 member economies have posted IAPs on the APEC website.[11]

III APEC CROSS-BORDER DATA TRANSFER

i Data Privacy Pathfinder Initiative

The APEC Privacy Framework does not explicitly address the issue of cross-border data transfer, but rather calls for cooperative development of cross-border privacy rules.[12] In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder Initiative with the goal of achieving accountable cross-border flow of personal information within the Asia-Pacific region. The Data Privacy Pathfinder Initiative contains general commitments leading to the development of an APEC Cross-Border Privacy Rules (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

8 See APEC Privacy Framework, paragraph 31.

9 See APEC Privacy Framework, paragraphs 40–45.

10 See APEC Privacy Framework, paragraph 39.

11 See www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx.

12 See APEC Privacy Framework, paragraphs 46–48.

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. Since 2008, the Data Privacy Subgroup has been working on nine interrelated projects to support the development of cross-border privacy rules in the Asia-Pacific region. Both the CBPR System and the CPEA are outcomes of the Pathfinder Initiative.

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 a newly established system, the CBPR System is in early stages of implementation. As of August 2014, three APEC economies participate in the CBPR System – Japan, Mexico, and the United States – with more expected to join (including Canada, which recently submitted a notice of intent to participate).

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.[13]

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.[14]

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is comprised 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 System Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.[15]

Accountability agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private

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

14 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.

15 See https://cbprs.blob.core.windows.net/files/JOP%20Charter.pdf and https://cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf.

accountability agents) or under applicable domestic laws and regulations (accountability agents and privacy enforcement authorities).

The CBPR System has its own website that includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports, and template forms.[16]

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 Cross-Border Privacy Enforcement Authority with at least one privacy enforcement authority;

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: (1) confirmation of CPEA participation; (2) identification of the APEC CBPR system recognised Accountability Agent that the economy intends to use; and (3) 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 such 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 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;[17]

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

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

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.[18]

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, then 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 continue to monitor certified organisations for compliance with the APEC CBPR System standards and must obtain annual attestations regarding such 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.[19]

As of August 2014, the CBPR System recognised only one accountability agent: TRUSTe, recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission.

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

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

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 August 2014, six organisations have been APEC CBPR certified, all of which are in the United States, with another 14 in various stages of review.[20] As more accountability agents are recognised in the economies participating in the CBPR System, the number of certified organisations is expected to grow.

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 in order to participate in the programme. With that exception, however, the CPBR 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 CPBR System, then those laws will continue to apply to their full extent.

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.

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

20 A current list of APEC-certified organisations can be found at www.cbprs.org/Business/BusinessDetails.aspx.

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 August 2014, CPEA participants included over two dozen Privacy Enforcement Authorities from eight APEC economies.[21]

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 CPBR 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 – the APEC Privacy Framework and the EU Data Protection Directive – in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In early 2014, the APEC/EU Working Group released a reference document (endorsed by APEC Senior Leaders in February 2014) that maps the CBPR System requirements and the Binding Corporate Rules under the EU Data Protection Directive, and identifies commonalities and differences between the two (the Referential).[22] This

21 See www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx for the most recent information about the CPEA and its participating privacy enforcement authorities.

22 See www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

document provides an important tool to multinational companies in developing global privacy compliance procedures that are compliant with both systems. Because it is set up in a block format, laying out the areas of commonality and the additional requirements of each privacy regime, the Referential provides a comparative tool that can be used as a checklist by companies seeking or considering certification by one or both systems. It does not, however, create interoperability or mutual recognition of the regimes.

The Referential points out that such companies still need to be approved by each of the respective bodies in both EU Member States and APEC economies. The Referential further cautions against using the document itself as an organisation's proposed framework because each organisation's privacy policies should be tailored to that organisation. Moreover, data processed in an APEC economy is still subject to that economy's domestic laws. And whenever the APEC CBPR System is incompatible with the EU Data Protection Directive, the organisation must affirmatively describe the circumstances under which it will apply the rules of one system rather than the other.

The Referential is one step toward developing policies, practices and enforcement procedures that could apply to both systems, and perhaps – eventually – a common framework.

V THE YEAR IN REVIEW AND OUTLOOK

The Data Privacy Subgroup is undertaking a 10-year review and evaluation (stocktake) of domestic and international implementation of the APEC Privacy Framework in 2014–2015 through a working group established for that purpose and led by Australia. The member economies have been encouraged to update their Data Privacy IAPs in support of that stocktake. The stocktake will consider whether the APEC Privacy Framework should be updated to ensure relevance as the market evolves with technology innovations, such as big data, cloud computing and the internet of things.

The United States (2012), Mexico (2013) and Japan (2014) became the first approved APEC Economies to participate in the APEC Cross-Border Privacy Rules System. TRUSTe became the first recognised Accountability Agent under the CBPR System on 25 June 2013. IBM became the first company to be certified under the APEC CBPR System in August 2013. Canada submitted its notice of intent to participate in the CBPR System in August 2014. Some commentators have anticipated that as many as five to 10 more economies will submit similar notices of intent in the next year.

APEC is developing a set of standards for cross-border transfers relating to data processors to complement the CBPR System (which applies only to data controllers).

Interoperability continues to be of significant interest. Following the publication of the Referential and in recognition of differences between the APEC CBPR System and the EU Binding Corporate Rules, additional documentation and checklists will be developed to provide a resource to companies seeking approval and certification under both systems.

A grant of surplus funds from the 2013 APEC Privacy Enforcement Workshop in Auckland, New Zealand permitted an expansion of the World Legal Information Institute's International Privacy Law Library. The Library contains the largest freely accessible searchable collection of privacy law materials in the world.

Appendix 1

ABOUT THE AUTHORS

CATHERINE VALERIO BARRAD

Sidley Austin LLP

Catherine M Valerio Barrad is a partner in the Los Angeles office of Sidley Austin LLP. She practises primarily in the area of privacy and data protection law, cross-border discovery issues, and consumer protection litigation including unfair and deceptive practices. She also represents clients in complex civil ligation, consumer class actions and appellate matters.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy, data security and information law 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 chairman 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 Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President. He is 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
555 West Fifth Street
Los Angeles, CA 90013
United States
Tel: +1 213 896 6000
Fax: +1 213 896 6600
cbarrad@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