Asia-Pacific
Economic Cooperation

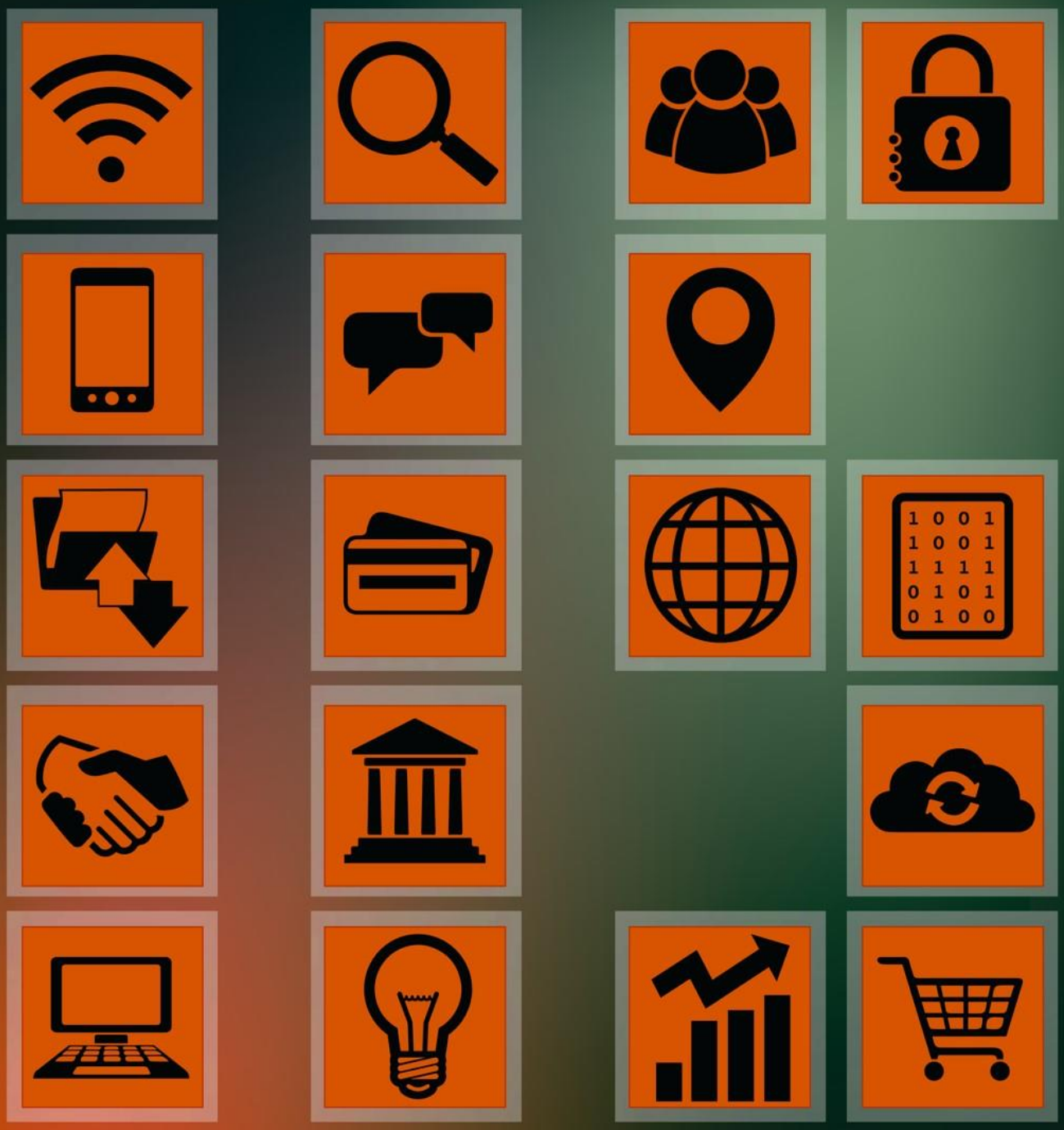
2014/SOM3/ECSG/DPS/004
Agenda Item: 2d

Report for APEC: Australia – Phase 1 – CBPR – Impediment Analysis

Purpose: Information
Submitted by: United States

APEC
CHINA 2014

Data Privacy Sub-group Meeting
Beijing, China
7 August 2014



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

INFORMATION INTEGRITY SOLUTIONS

building trust and
innovative privacy solutions

REPORT FOR APEC – AUSTRALIA – PHASE 1

CBPR – IMPEDIMENT ANALYSIS

16 JULY 2014

TABLE OF CONTENTS

1 APEC AND PRIVACY

Australia was among the first economies to join APEC in 1989. APEC's primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region. It also plays an important role in the Asia Pacific region to promote a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information. The first significant component of this effort was the APEC Privacy Framework and the second was the Cross border Privacy Enforcement Arrangement (CPEA). The most recent component of the framework is known as the APEC Cross Border Privacy Rules System (APEC CBPR) (APEC Cross-Border Privacy Rules System – Polices, Rules and Guidelines p.2, http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf).

Australia has been a leader in developing this process and currently has a representative on the Joint Oversight Panel, which is the Panel that makes recommendations to the Chair of the APEC Electronic Commerce Steering Group (ECSG) and APEC Member Economies regarding Member Economy and Accountability Agent participation in APEC CBPR (as discussed below) amongst other responsibilities as outlined in the Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.

2 CLIMATE IN AUSTRALIA TOWARDS PRIVACY

Australia has recently amended its privacy law. New Australian Privacy Principles (APPs) came into operation on 12 March 2014 after a long round of deliberations and consultations since the previous Act was reviewed by the Australian Law Reform Commission between 2006 and 2008. Greater enforcement powers have also been provided to the Privacy Commissioner.

In addition, Australia is now operating in a strong political climate of 'cutting red tape' as the government seeks to implement its deregulation agenda and track its commitment to cut $1 billion of red tape every year (http://www.cuttingredtape.gov.au/).

3 INTRODUCTION, OBJECTIVE AND OVERALL ASSESSMENT

The APEC Secretariat has contracted Information Integrity Solutions Pty Ltd (IIS) to provide a report identifying any impediments (legal or policy) and thus the ability and willingness of Australia to sign letters of intent to join APEC CBPR (Phase 1).

This report will be presented to the APEC Data Privacy Subgroup meeting in China in August 2014.

IIS has prepared this report based on its understanding of APEC CBPR and an intimate knowledge of privacy law in Australia. In addition, IIS has met with key government officials in Australia and the Australian Privacy Commissioner to seek their insights and perspectives.

The assessment and recommendations in this report are intended as general policy advice; they are not intended to be and should not be taken as legal advice.

The most significant elements of the report are those that identify and address impediments that may relate to the recognition of APEC Accountability Agents and the role of privacy enforcement authorities in the Australian context. The latter requirement also necessitates a high level gap analysis between the APEC Privacy Framework, in particular APEC CBPR procedural and intake

documents and the Australian Privacy Act. This analysis is necessary because one of the requirements of an economy wishing to join APEC CBPR is that it has a privacy enforcement authority capable of enforcing the obligations spelt out in the APEC CBPR procedural and intake documents for organisations wishing to join APEC CBPR.

A subsequent phase of the project will address any benefits that may arise to Australian consumers, business and government in signing up to APEC CBPR.

To date, three APEC economies have signed letters of intent to join APEC CBPR, namely USA, Mexico and Japan. We understand that other economies are considering joining. Companies that are now operating under APEC CBPR include IBM, Merck, Workday, Lynda and Yodlee.

IIS concludes that there are no legal impediments for Australia to join the CBPR, but there may be policy reasons that may affect the speed with which Australia signs letters of intent to join CBPR and the method chosen to ensure enforceability depending on whether a line by line or more principles based approach is adopted.

4 REQUIREMENTS AN ECONOMY MUST MEET IN ORDER TO PARTICIPATE IN APEC CBPR

The CBPR Policies, Rules and Guidelines note that in order to participate in APEC CBPR, an Economy must first satisfy the conditions in 2.2 of the Charter of the Joint Oversight Panel. The Economy then nominates one or more Accountability Agents for APEC recognition or notifies the ECSG Chair of receipt of application(s) for such recognition (http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf).

The conditions in 2.2 of the Charter specify that:

> "An APEC Member Economy is considered a Participant in the Cross Border Privacy Rules (CBPR) System (CBPR Participant), after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:
>
> i. The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);
> ii. The Economy indicates its intention to make use of at least one APEC recognized Accountability Agent subject to the procedures outlined in paragraph 6.2;
> iii. The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the Joint Oversight Panel, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and
> iv. The Joint Oversight Panel submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied."

5 AUSTRALIA HAS A PRIVACY ENFORCEMENT AUTHORITY THAT HAS JOINED THE CROSS BORDER PRIVACY ENFORCEMENT ARRANGEMENT

The first requirement Australia would need to meet in order to join APEC CBPR is that it has a Privacy Enforcement Authority in Australia that participates in the Cross Border Privacy Enforcement Arrangement. The Privacy Commissioner of Australia became a participant in 2010, thus satisfying this requirement. The full list of participants can be found on the APEC website at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

6 INTENTION TO RECOGNISE ACCOUNTABILITY AGENT

The second requirement Australia would need to meet would be to confirm its *intention* to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel. This requires that:

- "The applicant Accountability Agent has a location in a CBPR Participant's Economy or is subject to the jurisdiction of the relevant privacy enforcement authority in that Economy and;
- The applicant Accountability Agent meets the Recognition Criteria established under the CBPR System and has provided all necessary documentation as requested by the Joint Oversight Panel"

The Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel state that "the Economy need not name a specific Accountability Agent at this point, only affirm its intention to use the services of an APEC-recognised Accountability Agent once it has been identified and approved" (p.2).

The Accountability Agent Recognition Criteria are published at: http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.pdf.

In discussions with the Attorney-General's Department of Australia (AGD), staff noted that should Australia wish to join APEC CBPR, the Department's advice to the Attorney-General would need to include a recommendation to agree that Australia would make use of an APEC-recognised Accountability Agent which is subject to the jurisdiction of the relevant enforcement authority in Australia. AGD staff did not identify a legal impediment to providing such advice, rather it would be a policy question for the government to consider.

The Department of Foreign Affairs and Trade has indicated that it will support any position taken by the AGD.

7 HIGH LEVEL GAP ANALYSIS

In order for Australia to join APEC CBPR, the requirements of participating organisations have to be enforceable by privacy enforcement authoritie(s). This, therefore, necessitates a high level gap

analysis between the APEC privacy framework and, in particular, APEC CBPR procedural and intake documents and the Australian Privacy Act.

Generally APEC CBPR is more prescriptive than the APPs. The Australian Privacy Act, like many other jurisdictions, adopts principle based laws, which have the benefit of remaining relevant for longer as change accelerates, as well as being technology neutral.

The APPs, however, like APEC CBPR, take an accountability approach in relation to cross-border data transfers. According to the Explanatory Memorandum accompanying the Australian *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth):

> "there are currently two internationally accepted approaches to dealing with cross-border data flows: the adequacy approach, adopted by the European Union in the Data Protection Directive of 1996, and the accountability approach, adopted by the APEC Privacy Framework in 2004. NPP 9 was expressly based on the adequacy approach of the EU Directive. Under the new reforms, APP 8 and section 16C will introduce an accountability approach more consistent with the APEC Privacy Framework." (p.70)
> http://www.austlii.edu.au/au/legis/cth/bill_em/pappb2012476/memo_0.html

There do not appear to be inconsistencies between APEC CBPR and the APPs, rather APEC CBPR goes into further detail as to how one might implement collection, use, disclosure, security and other privacy principles. A few examples follow (this is a non-exhaustive list):

Definition of consent

If a use or disclosure of personal information is being made for a purpose unrelated to its collection, consent can be sought. In APEC CBPR that consent needs to be express (Q9). In the APPs consent can also be sought for uses and disclosures that are not related to their collection (APP 6), however by definition in section 6 of the Australian Privacy Act, consent can be express or implied (although the Information Commissioner's Guidelines suggest that an APP entity should generally seek express consent before handling 'sensitive' personal information. (Chapter B para B.35)).

Choice

APEC CBPR provides that where appropriate, individuals need to be provided with choice in relation to collection, use and disclosure of their personal information. The APPs do not speak in the language of 'choice' as such, but rather require entities to seek consent or fall within specified exceptions if they wish to use or disclose personal information for secondary purposes (APP 6.1). Hence, the provisions which provide 'choice' within the APPs are structured differently to APEC CBPR, though the intent is similar.

Security

APEC CBPR requires more prescriptive action to be taken in relation to the security of personal information obligations, such as security training; describing how safeguards are proportional to the likelihood and severity of harm threatened, sensitivity of information and context; and requiring an information security policy (Q26, 28 and 29). APP 11 governs the security of personal information and stipulates that reasonable steps be taken to ensure that personal information is protected from

misuse, interference and loss and from authorised access, modification or disclosure. APP 11 does not, however, specifically require, for example, an information security policy per se.

Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner (OAIC, which includes the Privacy Commissioner) stipulate that entities bound by the Privacy Act should consider whether they have "documented policies that address security matters, such as physical, ICT security and other appropriate information handling practices" (p. 25 Guide to information security: 'reasonable steps' to protect personal information, April 2013 http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security).

As such even though the Privacy Act does not impose such specific requirements across the board, they are clearly envisaged as responses to the broader intent of the security requirement in the Act. Indeed, a well specified security policy may be one of many things that Commissioner could require in response to a particular investigation to ensure effective security controls.

Integrity

APEC CBPR requires that where corrections are made to personal information, those changes need to be communicated to suppliers, such as processors, agents or other service providers to whom the personal information was transferred. Likewise, when those suppliers become aware of personal information that is inaccurate, incomplete or out of date they need to notify the entity bound by APEC CBPR. The correction principle (APP 13) only requires suppliers to be notified of corrections on request of the individual.

Person responsible for privacy

APEC CBPR require an individual to be responsible for overall compliance with the privacy principles (Q40). There is no express requirement for this under the APPs, rather there is an over-arching principle (APP 1.2) which addresses the need for a governed entity to implement practices, procedures and systems that will ensure the entity complies with the APPs and a registered APP code (if any) that binds the entity. The OAIC Guidelines on APP 1 in Chapter 1, Para 1.7 refer to a designated privacy officer as an example of a step that an entity could consider implementing to ensure compliance with APP 1 (http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/chapter-1-app-guidelines-v1.pdf).

Procedures for responding to judicial orders, subpoenas, warrants and other orders

APEC CBPR require procedures to be in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information (Q45). Under the Australian Privacy Act there are no specific procedures required, though disclosures may not breach the Australian Privacy Act if they fit 'authorised by law' tests, which expressly include Australian court/tribunal orders and which are defined in the Act as:

> "an order, direction or other instrument made by:
>
> (a) a court; or
> (b) a tribunal; or
> (c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or

(d) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or
(e) a member or an officer of a tribunal;

and includes an order, direction or other instrument that is of an interim or interlocutory nature."

That said, it may be that reasonable steps under APP1.2 could include internal policies dealing with responding to these situations.

Ensuring an organisation's service providers and others process personal information in line with its obligations

APEC CBPR require that mechanisms are in place with personal information processors, agents, contractors or other service providers pertaining to personal information they process on behalf of the APEC CBPR organisation to ensure that the APEC CBPR organisation's obligations to the individual will be met. These mechanisms may include contractual arrangements, policies, compliance with relevant industry standards and so forth. While there are no such specific requirements in the Australian Privacy Act, an organisation operating in Australia providing such services is bound by the provisions of the Act anyway unless is exempt from the Act (for example because it is an exempt small business). That said, the OAIC guidelines note that an organisation that is 'outsourcing' within Australia would need to take reasonable steps under APP1.2 to protect the information affected by the outsourcing for example "mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs". (Chapter 1, para 1.7 of the Guidelines).

In relation to offshore providers APP 8 requires that before an organisation sends information offshore, it "must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1)", unless exceptions apply (essentially because other protections are in place).

Gap analysis conclusion

Discussions with the OAIC have indicated that it would not be able to enforce directly specific prescriptive provisions in APEC CBPR such as those identified here, where there are no such requirements in the APPs unless OAIC concluded that the absence of their implementation by an organisation had led to a breach of one of the APPs. For example, an organisation with a weak privacy framework may not meet the requirements of APP 1.2 in a circumstance where deploying a privacy officer might be seen as the way to address the deficiency.

8 LINE BY LINE OR PRINCIPLES BASED APPROACH TO MEETING REQUIREMENTS IN THE CHARTER OF THE JOINT OVERSIGHT PANEL?

In accepting proposals to participate from previous economies, the Findings Reports of the Joint Oversight Panel have taken a principles based approach to considering whether an economy wishing to participate in APEC CBPR meets Charter requirements. The successful submissions by Japan and Mexico to the Joint Oversight Panel outline at a high level where equivalent privacy principles match APEC CBPR.

The assessment in this report indicates that if a similar approach is taken in regard to Australia, it would meet Charter requirements along with those economies already participating based on the Privacy Act as it currently stands.

However, in the Australian context, the specific prescriptive provisions of APEC CBPR could become more explicitly enforceable through two potential avenues, namely the adoption of a binding code or a co-regulatory approach with the Australian competition regulator, the Australian Competition and Consumer Commission, which are discussed below.

9 CODES

Part IIIB of the Privacy Act deals with the development of privacy codes. Codes may be developed in a range of circumstances as outlined in the OAIC's Guidelines for Developing Codes - Issued under Part IIIB of the *Privacy Act 1988*, in September 2013.

As outlined in those Guidelines,

> "The primary purpose of an APP code is to set out how one or more of the APPs are to be applied or complied with. An APP code may also impose additional requirements to those in the APPs and/or cover certain exemptions. As such, reasons for developing an APP code may include:
>
> - providing greater clarity of how particular APPs are applied or complied with in a specific industry context or in relation to new and emerging technologies which entities bound by the code utilise
> - incorporating higher standards for privacy protection than the Privacy Act requires, including covering certain exempt acts or practices or providing for additional obligations to those in the APPs or Part IIIA (For example as outlined in footnote 6 of the Guidelines, this would allow entities and industries which operate in overseas jurisdictions, where higher privacy standards apply, to match those higher standards in their Australian operations.)
> - assisting in promoting cultural change in an industry sector in relation to personal information handling."
> http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/guidelines-for-developing-codes

As such, since APEC CBPR and APPs are principally pursuing the same obligations, with APEC CBPR expanding in further detail what this may specifically entail, the development of a code replicating the further requirements would fit well within the purposes of the code development provisions in the Australian Privacy Act. This was further reinforced with discussions with the OAIC and the AGD.

A code can be developed at the Privacy Commissioner's request or by an 'APP code developer'. An APP entity, group of APP entities or a body or association representing APP entities can develop a code, as defined by the term 'APP code developer'. The first binding code that has been developed under the amended Australian Privacy Act in 2014 is the Credit Code, which the Act required to be developed to apply to credit providers and credit reporting bodies.

It is important to note that the Privacy Act has a number of exemptions, but some of the normally exempt entities or practices may become regulated through a binding Code. For example,

section 26(C)(3)(b) provides that a code may cover an act or practices that is exempt under the meaning of section 7B(1)(2) or (3). These provisions relate to:

- Individuals acting in a non-business capacity
- Contracted service providers to Commonwealth and State contracts (though some reservations as outlined in section 6B where Commonwealth contracts are inconsistent with the provisions of the Code)
- Employee records; and
- Journalism

A small business, which is also not normally regulated under the Privacy Act, may be bound by a Code if it has opted-in to be bound by the Privacy Act in the first instance, pursuant to section 6EA of the Australian Privacy Act. Political entities, however, under current law, will never be bound by the Australian Privacy Act or a binding code. It should be noted that political entities, in any event, cannot be part of APEC CBPR, as the latter is only intended to cover commercial entities, so this is not an impediment.

As mentioned in the opening paragraphs of this report, it is worth noting that in the current political climate in Australia there is strong emphasis on 'cutting red tape' where possible and ensuring that any new regulatory impacts or burdens are assessed with a lens that takes into consideration the government's mandate to reduce regulatory burden for individuals, businesses and community organisations ("The Australian Government Guide to Regulation", Department of the Prime Minister and Cabinet, 2014, in particular p. 4; http://cuttingredtape.gov.au/handbook/australian-government-guide-regulation). As such, before the Privacy Commissioner could make a code binding and hence enforceable, a Regulation Impact Statement (RIS) would need to be conducted and signed off by, in this case, the Privacy Commissioner. The requirements for conducting a RIS are outlined in the Guide and include consultations with relevant stakeholders.

Facilitative regulation that enables trade whilst protecting personal information is unlikely to be viewed as 'red tape' in the context of a RIS. One of the main purposes of adopting a major regional privacy standard, such as APEC CBPR is to 'enable global organizations that collect, access, use or process data in APEC Economies to develop and implement uniform approaches within their organizations for global access to and use of personal information'.

Additionally, since a Code would simply be a process whereby APEC CBPR could be adopted, this arguably does not add regulatory burden. The Australian Government Guide to Regulation states on page 29 that "if any of the options involve establishing or amending standards in areas where international standards already apply, you should document whether (and why) the standards being proposed differ from the international standard".

Finally and importantly, the voluntary nature of the Code means that only businesses that see benefit in doing so will participate.

Discussions with AGD indicated that should the Government decide to seek participation in APEC CBPR, options that the government would need to consider would include whether Australia should take a similar approach to the submissions that were lodged by Mexico and Japan and accepted by

the Joint Oversight Panel or whether a more prescriptive approach should be taken and if so, whether a Code would be the best way of doing so.

10 COMPETITON AND CONSUMER REGULATION

Discussions with the Privacy Commissioner revealed a possible alternative approach, namely a joint regulatory approach between the Privacy Commissioner and the Australian Competition and Consumer Commission (ACCC), which has oversight and regulatory powers in relation to misleading and deceptive conduct under the *Competition and Consumer Act 2010* (Cth), much like the Federal Trade Commission in the United States.

If this alternative stood up against further detailed analysis and was agreeable to both the ACCC and the Privacy Commissioner, a Memorandum of Understanding may be required between the regulators. It would address those aspects of APEC CBPR that are not enforceable under the Privacy Act, due to their level of prescription and recognise that they may be enforceable by the ACCC if an entity agrees to abide by APEC CBPR, but in practice does not, and accordingly arguably engages in misleading and deceptive conduct. Other provisions equivalent to the APPs would remain within the jurisdiction of the Privacy Commissioner.

In order for this to meet the requirements for Australia to join APEC CBPR, the ACCC, would then also need to become a privacy enforcement authority that has joined the CPEA, being a 'public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. 'Privacy Law' is 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' p.10).

Whilst IIS has not discussed this with the ACCC, the AGD noted that the ACCC does not position itself as a 'consumer affairs bureau', because it largely deals with big business issues, not individual consumer rights. It is the fair trading bodies in the Australian States that deal with consumer issues.

As such, the adoption of a Code would be the better approach, should Australia wish to take more of a line by line approach.

11 OVERALL ASSESSMENT

IIS concludes that there are no legal impediments for Australia to join the CBPR, but there may be policy reasons that may affect the speed with which Australia signs letters of intent to join CBPR and the method chosen to ensure enforceability depending on whether a line by line or more principles based approach is adopted.

12 APPENDIX – CONSULTATIONS

Malcolm Crompton, Managing Director and Annelies Moens, Head of Sales and Operations at Information Integrity Solutions Pty Ltd held discussions and meetings with the following government departments and Privacy Commission in June 2014:

Organisation	**Staff**
Office of the Australian Information Commissioner	• Timothy Pilgrim, Privacy Commissioner of Australia • Angelene Falk, Assistant Commissioner Regulation and Strategy Branch • Andrew Solomon, Director Privacy Law and Practice
Attorney-General's Department	• Andrew Walter, Assistant Secretary, Commercial and Administrative Law Branch • Wanni Teo, Acting Principal Legal Officer
Department of Communications	• Keith Besgrove, First Assistant Secretary, Digital Services Division • Duncan McIntyre, Assistant Secretary, Consumer Policy and Post • Tristan Kathage, Director, Cloud Computing and Privacy Section, Consumer and Post Branch • Jen Watson
Department of Foreign Affairs	• Heath McMichael, Senior Adviser, trade and economic policy, APEC Branch

Information Integrity Solutions Pty Ltd
Level 3, 53 Balfour Street, Chippendale, Sydney NSW 2008 Australia
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898

INFORMATION INTEGRITY SOLUTIONS

building trust and
innovative privacy solutions