



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 9PVLR1444, 10/18/2010 . Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### **APEC Roundup: Update on Accountability Agents in Implementation Of the APEC Framework, Development of Pathfinder Projects, More**



BY PAULA J. BRUENING

In 2010, work on issues related to the practical implementation of the Asia Pacific Economic Cooperation (APEC)<sup>1</sup> Privacy Framework continued at meetings in Japan. The Data Privacy Subgroup of APEC's Elec-

<sup>1</sup> APEC is a forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region. It op-

*Paula J. Bruening is Deputy Executive Director of The Centre for Information Policy Leadership at Hunton & Williams LLP in Washington. Bruening focuses on cross border data flows, emerging technologies, government use of private sector data and cybersecurity issues.*

tronic Commerce Steering Group—the body tasked with addressing privacy at APEC—convened in Hiroshima in February and Sendai in September. Their work focused on exploration of the role of accountability agents in the implementation of the APEC Framework, further development of Pathfinder Projects, and the monitoring of developments in data protection regimes in participating APEC economies. The work of data privacy subgroup will continue as APEC moves to the United States in 2011 to hold meetings in Washington and San Francisco.

#### **What Is the APEC Privacy Framework?**

The APEC Privacy Framework<sup>2</sup> is a practical approach to facilitating the protected flow of data throughout the region. It establishes accountability in the flow of data while preventing impediments to data transfer. It provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspective. The Framework provide clear guidance and direction to businesses in APEC member economies on common privacy issues and proposes reasonable expectations of how information should be protected.

The Framework takes into consideration both domestic and international implementation of privacy standards for APEC member economies. It is designed to facilitate information sharing and cooperation across

erates on the basis of non-binding commitments. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

<sup>2</sup> <http://op.bna.com/pl.nsf/r?Open=dapn-8a7vyl>

agencies and authorities to enable transfers of personal information across borders. The Framework also provides specific examples of privacy situations and focuses on practical and consistent information privacy protection.

The nine principles of the APEC Privacy Framework are:

- Preventing harm;
- Notice;
- Collection limitation;
- Use of personal information;
- Choice;
- Integrity of personal information;
- Security safeguards;
- Access and correction;
- Accountability.

Thirteen APEC member economies have agreed to the development of this framework for flows of personal data across the region.<sup>3</sup>

The principles balance privacy with other relevant interests, recognizing the diverse attitudes about privacy that exist within the region. The principles further take into account the disparity among economies with respect to their privacy protection regimes. In some cases data protection laws, self-regulation and enforcement are well developed; other economies may have no established protections for data privacy. The APEC Framework is designed to further protect, unencumbered data flows across this varied cultural, economic and legal landscape. Governments in APEC economies create an environment for data protection and the underlying mechanisms necessary to participate in cross-border data transfers. Regulations establish the obligations

The Framework principles are implemented through the operation of cross-border privacy rules and overseen by accountability agents. Under the APEC Framework, the obligations set out in the cross-border privacy rules travel with the data as it is transferred within the region and must be met by any entity that stores or processes that data. Cross-border privacy rules (CBPR), developed by companies in keeping with the APEC principles, establish their specific obligations to protect information and mechanisms to ensure that rules are enforced as data moves within the region. Accountability agents review the mechanisms created by companies to ensure that the objectives of the APEC Privacy Framework are met as data is transferred within organizations.

When the consumer believes that his or her data has been mishandled or that promises made with respect to the handling and protection of the data have not been met, the APEC Framework provides for the operation of accountability agents as the consumer's first line of recourse. Accountability agents may be government bodies or independent third parties. Such a system would afford the consumer protection for his or her data, and

<sup>3</sup> The word economies is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues. Members engage with one another as economic entities. The APEC members include Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Viet Nam.

a local system for recourse that does not entail tracking of data outside of one's home economy.

The Framework and the Principles were endorsed by the APEC Ministers in 2004. Since then, work has centered on close examination of the details of the principles and mechanisms essential to the practical operation of the Framework.<sup>4</sup>

## Accountability and the APEC Framework

The Accountability principle provides that

[a] personal information controller should be accountable for complying with measures that give effect to the Principles . . . When personal information is to be transferred. . . whether domestically or international, the personal information controller should obtain the consent of the individual or exercise due diligence and take responsible steps to ensure that the recipient . . . will protect the information consistently with those Principles.<sup>5</sup>

Recognizing that efficient and cost-effective business models often require transfer of information between different types of organizations in different locations, the principles require that personal information controllers should be accountable for ensuring that the recipients should take conduct due diligence and take reasonable steps to ensure the information is protected consistent with the APEC Principles, even after it is transferred. Thus according to the Principles, the obligations to protect the data travel with it, and the data controller is accountable for its protection no matter where or by whom it is processed, except where domestic law requires its disclosure for specified purposes.

Much of the work in Japan focused on the nature and role of accountability agents in the practical implementation of the principles. In the APEC Framework, accountability agents would ensure that companies asserting they are accountable under its terms can in fact fulfill their obligations to protect, process and store data properly. They would also serve as clearinghouses for resolution of disputes that may arise in cross-border data transfers. Critical to their role would be their ability to resolve disputes raised by individuals who may require their assistance, particularly when data has been transferred to a distant jurisdiction. Participants in the Japan meetings included business representatives, government agencies and privacy experts. They explored the possible roles of auditors, law firms or consulting firms as accountability agents, and evaluated each organization in that role. They also considered the need for cross-recognition between accountability agents in and APEC CBPR system, and the relationship between accountability and government regulators.

## The Pathfinder Projects

To facilitate implementation of the APEC Privacy Framework, the Electronic Commerce Steering Group developed the Pathfinder initiative. The Pathfinder fa-

<sup>4</sup> For example, a workshop was conducted in Mexico City in May 2007 to come to a better understanding of the role and function of accountability agents, and in particular trustmarks, throughout the APEC region. That workshop also explored the common criteria necessary to ensure credibility of accountability agents across economies.

<sup>5</sup> APEC Privacy Framework, Principle 9, at <http://op.bna.com/pl.nsf/r?Open=dapn-8a7vyl>.

cilitates collaboration among APEC member economies on development and testing of the practical element of a system that would enable cross-border data flows under the guidance of the APEC principles. Among the Pathfinder's objectives are (1) to promote a consultative process that includes all stakeholders in both the creation and review of the rules and processes; and (2) to explore ways in which various documents and procedures may be practically implemented in a manner that is flexible, credible, and enforceable.

Participating economies agreed on nine collaborative project to develop tools, resources, and supporting mechanisms that further implementation. The projects also provide opportunities to test the complaint resolution process and the reviews by government suggested by the APEC Framework and Principles. Work on the pathfinder projects is conducted in the periods between APEC meetings. If successfully carried out, the projects will lead to a system for implementation for the APEC cross-border data rules.

The Pathfinder projects include:

#### **Project 1: Self-assessment guidance for businesses**

This document will guide companies in conducting an internal review of their data practices that will further implementation of CBPRs.

#### **Project 2: Trustmark guidelines.**

This project develops the criteria by which private (non-governmental) accountability agents wishing to participate in the APEC CBPR will be evaluated. Guidelines will be designed to ensure the accountability agent's independence and its ability to render a fair decision. The guidelines address dispute resolution procedures, compliance review and enforcement.

#### **Project 3: Compliance review process of CBPRs**

This project develops guidelines for use by accountability agents when reviewing an organization's cross-border privacy rules and assessing its compliance with the APEC Privacy Principles.

#### **Project 4: Directories of compliant organizations**

This project develops a publicly accessible director of organizations whose CBPRs have been recognized as complying with the APEC Privacy Principles. The directory will also include contact information for organizations and relevant accountability agents.

### **5. Contact directories of data protection authorities and privacy contact officer**

The project will establish and maintain a directory of relevant data protection authorities or privacy contact officers in APEC economies. Such a directory will help data protection authorities and privacy contact officer locate appropriate counterparts when necessary to address a cross-border privacy complaint.

### **6. Templates for enforcement cooperation agreements**

This project will develop cooperative arrangements between relevant enforcement authorities that will facilitate the exchange of information and foster cross-border cooperation in investigation and enforcement.

### **7. Templates for cross-border complaint handling forms**

This project develops a template for use by relevant data protection authorities to determine the appropriate course of action in providing investigative assistance.

### **8. Guidelines and procedures for responsive regulation in CBPRs' systems**

This project will develop guidelines and procedures to assist in determining at which stage a cross-border complaint should be handled and identify the triggers for escalating a complaint.

### **9. Implementation pilot program**

This project serves as a test-bed for implementation of the results of the various projects.

## **Privacy Developments in Participating APEC Economies**

### **Chile**

Currently, Chilean law does not provide express privacy protections for private sector commercial transactions. Moreover, no Chilean regulatory entity is chartered to enforce such protections. A proposed amendment to Chile's 1998 Privacy Law would address protection of data in commercial transactions consistent with the APEC Privacy Framework and establish a privacy enforcement authority. Under the proposed amendment, a special government council would enforce the privacy protections enumerated in the proposed amendment, including the regulation of cross-border data flows. Should the amendment be enacted, Chile would most likely make use of a public-sector accountability agent.

### **Vietnam**

While various elements of privacy law are already in place in Vietnam's law on E-Transactions (2005), the Vietnamese General Assembly is considering a comprehensive consumer privacy law. Article 4 of the draft law, entitled "Protection of Consumers' Privacy," imposes requirements on businesses that correspond to those outlined in the APEC Privacy Framework. It has established a national trustmark that can serve as an accountability agent, Trust VN, as a subunit within their e-Commerce and IT Agency. A final decision as to the appropriate enforcement authority has not yet been made.

Vietnam's recently adopted "Master Plan on e-Commerce Development for the Period 2011-2015" reflects the economy's extensive involvement in work on the APEC Pathfinder project. The Plan recommends that "[s]tate Agencies review, supplement, amend, and promulgate new policies and legal texts to give support and create favorable conditions for the e-commerce development, including: Legal texts ensuring that personal information in e-transactions are legally protected according to international standards and Vietnam's international commitments."

### **Indonesia**

While Indonesia does not have in place an overarching privacy law, its "Law Number 11 of 2008 on Electronic Information and Electronic Transactions" establishes a general privacy right. The law provides for government implementation of regulations that would further define this privacy right in accordance with the system of privacy rules under development at APEC. Such implementing regulations, including "Provisioning Electronic Information and Transaction" and "Protecting Strategic Data," are currently under development. Indonesia is contemplating a government-

sponsored accountability agent in which the private sector participates. The Ministry of Trade or Ministry of Information Tech and Communications will likely serve as the enforcement authority.

### **The Philippines**

The Philippine Legislature is currently considering legislation that would protect the privacy of Philippine citizens and create an environment conducive to outsourcing. While proposed legislation was not voted on before adjournment of the Philippine's last Congress, the same bill was introduced before the current session and is likely to be approved. Policy makers in the Philippines anticipate that private sector entities will serve as accountability agents and is considering their possible accreditation through the Department of Trade and Industry (DTI). All enforcement will be a government function. DTI will likely be designated the government enforcement authority, either through presidential decree or by regulation.

### **Australia**

Australia released an "exposure draft" of what will be called the Australian Privacy Principles.<sup>6</sup> This release represents the beginning of a public consultation about the proposed revision and restructuring of Australia's privacy legislation. The Australian Privacy Principles would replace the existing Information Privacy Principles, which apply to Australian commonwealth

---

<sup>6</sup> <http://www.smos.gov.au/media/2010/docs/Privacy-reform-exp-draft-part-1.pdf>.

agencies, and the National Privacy Principles, which apply to certain private sector organizations. Principle 8—"Cross Border Disclosure of Personal Information"—would allow cross-border transfer or disclosure of data if the recipient is bound by adequate protections such as equivalent laws, contracts, self-regulation or "international arrangements that provide the necessary level of protection" for the data. It further requires that individuals have access to an enforcement mechanism, and makes the organization making the disclosure accountable for the data protection practices of the recipient.

### **New Zealand**

New Zealand's Law Commission has proposed changes to the Privacy Act that include an accountability similar to those found in international data protection statutes and guidelines. The New Zealand Privacy Commissioner has backed those changes, stating that an accountability principle could provide a measured response to the risks raised by the transfer of information into and out of the jurisdiction.

### **Looking Ahead**

At APEC meetings in the United States next year, the Data Privacy Subgroup's work will focus primarily on further development of the governance mechanisms that support CBPRs. The issues to be resolved include the scope of authority for bodies enforcing CBPRs, guidelines for complaint handling and escalation, and plans for implementation. The Data Privacy Subgroup will work toward endorsement of the results of all of the Pathfinder projects at the November 2011 meeting, with a goal of making the CBPR system operational in 2012.