

Reproduced with permission from Privacy & Security Law Report, 11 PVLR 2, 01/16/2012. Copyright © 2012 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## Cross-Border Data Transfers

### APEC Privacy Initiatives

## APEC Passes Privacy Policy Milestones, New Challenges Await in 2012



By PAULA J. BRUENING

**O**n Nov. 13, 2011, Asia-Pacific Economic Cooperation (APEC) leaders endorsed the APEC Cross-border Privacy Rules (CBPR) system<sup>1</sup> at an APEC meeting in Honolulu, Hawaii (10 PVLR 1673, 11/21/11).

<sup>1</sup> Organizations that participate in the CBPR system implement privacy policies and practices consistent with CBPR program requirements for all personal information they have collected or received that is subject to cross-border transfer to other participating APEC economies. An APEC-recognized accountability agent will evaluate these privacy policies and procedures to assess their compliance with the CBPR program requirements. Once an organization has been certified for participation in the CBPR system, these privacy policies and practices will become binding. For an in-depth discussion of CBPRs, see “APEC CBPR System—Policies, Rules and Guidelines,” at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_009.pdf](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf).

*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.*

The Leaders’ Statement also endorsed interoperability between national and regional privacy and data protection regimes that would facilitate moving data around the globe while protecting privacy.

APEC foreign and trade ministers issued a statement endorsing not only the CBPRs, but also the broader APEC Privacy Framework<sup>2</sup> of which they form an integral part. The statement further endorsed the principle documents of the APEC Data Privacy Pathfinder, which promote “regional economic, integration, regulatory cooperation, and cross-border trade.”

Commissioner Edith Ramirez of the Federal Trade Commission welcomed the initiative on behalf of the agency, noting the significant consumer protection issues raised by the global flow of data. U.S. Commerce Secretary John Bryson applauded the completion of the CBPR system, stating that the voluntary rules will promote a baseline set of data privacy practices for companies doing business in participating APEC economies.

In December, APEC also announced that an additional 15 authorities from Japan had joined the APEC Cross-border Privacy Enforcement Arrangement. The 15 Japanese authorities<sup>3</sup> join five authorities from Aus-

<sup>2</sup> The Framework is comprised of a set of nine guiding principles and guidance on implementation to assist APEC Economies in developing consistent domestic approaches to personal information and privacy protections. It forms the basis for development of a regional approach to promote accountable and responsible transfers of personal data between APEC economies. The nine principles include: Preventing Harm; Notice; Collection Limitations; Uses of Personal Information; Choice; Integrity of Personal Information; Security Safeguards; Access and Correction; and Accountability. A complete review of the APEC Privacy Framework can be found at <http://op.bna.com/pl.nsf/r?Open=dapn-8q8nf7>.

<sup>3</sup> The authorities from Japan that have been formally accepted as Privacy Enforcement Arrangement participants are: the Cabinet Office; Consumer Affairs Agency; Financial Services Agency; Ministry of Agriculture, Forestry and Fisheries; Ministry of Defense; Ministry of Economy, Trade and Industry; Ministry of Education, Culture, Sports, Science and Technol-

tralia, Canada, Hong Kong, New Zealand and the United States.<sup>4</sup> The Privacy Enforcement Arrangement represents a process that facilitates information sharing among privacy enforcement authorities in APEC economies; provides mechanisms to promote effective cross-border cooperation between authorities in the enforcement of privacy laws; and encourages information sharing and cooperation on privacy investigation and enforcement with privacy enforcement authorities outside APEC. The Privacy Enforcement Authority creates a framework for voluntary information sharing and for providing assistance among participating authorities for activities related to enforcement. Any privacy enforcement authority in an APEC economy may participate. Participating privacy enforcement authorities will contact each other for assistance or to make referrals regarding information privacy investigations and enforcement matters that involve each other's economies.<sup>5</sup>

While these developments are especially important for companies doing business in the Asia Pacific region—an area experiencing dynamic growth and the potential for expanded trade—they also come at a time when privacy and data protection policy is poised for significant reconsideration and revision. The European Commission is scheduled to release its proposed data protection regulations Jan. 25, 2012. Privacy policymakers and practitioners anticipate the release early in the year by the Department of Commerce of its white paper articulating U.S. privacy policy.<sup>6</sup> The Organisation for Economic Cooperation and Development has embarked on an inquiry into whether and how its Guidelines<sup>7</sup> might be revised. Endorsement of the Framework and CBPRs clears the way for discussions about how diverse privacy and data protection regimes can interoperate to facilitate the movement of data around the

ogy; Ministry of Environment; Ministry of Finance; Ministry of Foreign Affairs; Ministry of Health, Labor and Welfare; Ministry of Internal Affairs and Communications; Ministry of Justice; Ministry of Land, Infrastructure, Transport and Tourism; and the National Police Agency.

<sup>4</sup> The Federal Trade Commission is the authority participating in the Privacy Enforcement Arrangement from the United States.

<sup>5</sup> For example, during an investigation, a privacy enforcement authority in economy A may seek the assistance of a privacy enforcement authority in economy B, if certain evidence of the alleged privacy violation (or the entity being investigated) is located in economy B. In that case, the privacy enforcement authority in economy A may send a request for assistance to the point of contact in the privacy enforcement authority in economy B. The privacy enforcement authority in economy B may then consider the matter and provide assistance on a discretionary basis. For a complete discussion of the Cross-border Privacy Rule Enforcement Arrangement, see "APEC Cooperation Arrangement for Cross-border Privacy Enforcement," 2010/SOM1/ECSG/DPS/013, at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_010.pdf](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf).

<sup>6</sup> The Department of Commerce's preliminary green paper, "Commercial Data Privacy and the Internet Economy: A Dynamic Policy Framework," was released for public comment Dec. 16, 2010. The green paper is available at [http://www.ntia.doc.gov/files/ntia/publications/iptf\\_privacy\\_greenpaper\\_12162010.pdf](http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf).

<sup>7</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html).

world. The specific endorsement of interoperability by APEC leaders opens the door for APEC constituent economies and the European Commission to discuss how CBPRs and EU Binding Corporate Rules can be made to interoperate.

## The Pathfinders

The Privacy Enforcement Arrangement is the result of work on the APEC Pathfinders, embarked upon by the Data Privacy Subgroup<sup>8</sup> and participating APEC economies. The Pathfinders were designed as multi-year projects that would create the practical infrastructure for the implementation of the APEC Privacy Framework and the operation of the CBPRs.<sup>9</sup> In creating the Pathfinders, the participants in the work at APEC identified the three stakeholder concerns to be addressed:

- *organizations* should be able to trust that organizations with which they do business and enter into transactions that involve personal information have appropriate policies and procedures in place. These should be consistent with the APEC principles and respect applicable privacy and data security laws, as well as representations made to the individual when the personal information was collected;
- *consumers* should be able to trust that their personal information is secured when transferred across borders; and
- *governments* should eliminate unreasonable impediments to cross-border data transfers. At the same time, they should protect the privacy and security of citizens' personal information domestically and, in cooperation with foreign governments, internationally.

The Pathfinders resulted in several core instruments:

1. A *detailed self-assessment questionnaire*<sup>10</sup> for use by an organization applying for recognition as compliant with the APEC Privacy Principles.

The CBPR system relies on an organization's self-assessment of their data privacy policies and practices against the requirements of the APEC Privacy Framework.<sup>11</sup> The Pathfinder developed a questionnaire recognized by APEC. This questionnaire will be provided to the organization by an APEC recognized accountability agent, which will then review the completed documentation against baseline standards established in the

<sup>8</sup> The Data Privacy Subgroup is a working group of the APEC Electronic Commerce Steering Group (ECSG). The ECSG promotes the development and use of electronic commerce by fostering legal, regulatory and policy environments in the APEC region that are predictable, transparent and consistent.

<sup>9</sup> For further discussion of the Pathfinders, see "APEC Data Privacy Pathfinder Projects: Implementation Work Plan," at <http://op.bna.com/pl.nsf/r?Open=dapn-8q8nge>.

<sup>10</sup> "APEC CBPR System—Intake Questionnaire," 2011/SOM3/ECSG/DPS/005, at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_005.doc](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_005.doc).

<sup>11</sup> The requirements of the Framework are articulated in detail in the APEC CBPR Program Requirements Map, found in "APEC CBPR System—Accountability Agent Recognition Criteria," Annex C, 2011/SOM3/ECSG/DPS/006, at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_006.doc](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_006.doc).

CBPR program requirements. This step is the first in an evaluation that will determine whether the organization's privacy policies and practices are consistent with the program requirements of the CBPR system. An organization found to have fulfilled CBPR program requirements by an APEC-recognized accountability agent will be certified as CBPR compliant and will have their certification published on an APEC-hosted website so that consumers and other stakeholders can be aware that the organization actively participates in the CBPR system.

2. *The criteria to be applied by economies when evaluating an accountability agent applying for APEC recognition.*<sup>12</sup>

Work on the Pathfinder also resulted in an Accountability Agent Recognition Criteria Checklist. The completion of the document requires consideration of the following factors: the possible existence of a conflict of interests; the agent's program requirements; its certification process; its monitoring and compliance review processes, re-certification and annual attestation, dispute resolution process, and mechanisms for enforcing program requirements.

3. *The provisions of the Cross-border Privacy Enforcement Arrangement.*<sup>13</sup>

As discussed earlier in this article, accountability agents and privacy enforcement authorities will enforce the CBPR system. Accountability agents will enforce the CBPR program requirements through law or contract. Privacy enforcement authorities will be able to initiate enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements.

4. *The Charter of the Cross-border Privacy Rules Joint Oversight Panel.*<sup>14</sup>

The charter sets forth the conditions under which an organization can participate in the Cross-border Privacy Rules System and the role of the Joint Oversight Panel. It provides for transparency of the process and establishes how a participant can cease engagement in the CBPR system. It also sets forth the situations when an APEC economy's participation in the CBPR system may be suspended or terminated by other APEC economies. It establishes the Joint Oversight Panel, articulating its makeup and functions. Among the functions of the Joint Oversight Panel are consulting with economies that have indicated an intention to participate in the CBPR system and reporting on how the economy has met the necessary conditions; recommending to the APEC economies whether they recognize an applicant accountability agent as compliant with the requirements of the CBPR system; and considering and recommending suspension of an accountability agent's recognition. It articulates the processes by which it will make

recommendations, and how administrative matters will be handled.

## Looking Ahead to 2012: Governance of the CBPR System

When meetings move to Russia this year, APEC's work on privacy enters a new phase. The Pathfinders completed, efforts turn to development of a model for the effective administration of the CBPR system, bearing in mind the goal of keeping the system simple, transparent, low-cost and accountable to APEC economies.

Essential administrative functions would include:

- Developing and maintaining the staffing and revenue infrastructure necessary to support the CBPR System;
- Managing the APEC-hosted compliance directory;<sup>15</sup>
- Facilitating participation in the CBPR System by APEC Economies, including through capacity-building activities;
- Assessing and monitoring the compliance of recognized Accountability Agents against the recognition criteria;
- Managing the Cross-border Privacy Enforcement Arrangement and associated documents and procedures; and
- Developing education materials to facilitate an understanding of the CBPR System and its program requirements within the APEC region.

Perhaps the greatest task in developing this governance is the creation of a funding model that would support necessary activities. Governance of the CBPR system must be self-sustaining, and identifying the appropriate source of financial support that would function long-term—particularly at a time of scarce resources—will require creativity. Furthermore, the compliance assessment, information sharing and collaborative enforcement activities necessary to the success of the CBPR system will require an infrastructure based on trust among data protection authorities and accountability agents. Establishing and maintaining that trust will be essential, and it will be necessary to find ways to reassure participants in the CBPR system of the trustworthiness of their partners. Finally, this phase of the work will be carried out in a busy year for policymakers, as the European Union, the OECD, and the U.S. Department of Commerce continue their own important initiatives in privacy and data protection. Harnessing the resources of policymakers to address the work of each of these forums in a productive way will be its own challenge.

Participants in work on privacy at APEC begin this next phase at meetings in Moscow beginning Jan. 30. In spite of these challenges, they take important steps to

<sup>12</sup> "APEC CBPR System—Accountability Agent Recognition Criteria," 2011/SOM3/ECSG/DPS/006, [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_006.doc](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_006.doc).

<sup>13</sup> "APEC CBPR System—Policies, Rules and Guidelines," 2011/SOM3/ECSG/DPS/006, [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_009.pdf](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf).

<sup>14</sup> The Joint Oversight Panel will establish the authority for the operation of the CBPR system. The Charter may be found in "APEC Cross-border Privacy Rules System: Policies, Rules and Guidelines," 2011/SOM3/ECSG/DPS/009, at [http://aimp.apec.org/Documents/2011/ECSG/DPS2/11\\_ecsg\\_dps2\\_009.pdf](http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf).

<sup>15</sup> An organization that is found to be compliant with the CBPR program requirements by an APEC-recognized Accountability Agent will be certified as CBPR compliant and will have relevant details of their certification published in an APEC-hosted website so that consumers and other stakeholders can be made aware that the organization is an active participant in the CBPR system.

ward making the APEC Framework a practical reality for organizations and privacy and data protection au-

thorities, and toward facilitating the protected movement of data around the globe.