

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

## OVERVIEW

**The Problem.** The rise of the Internet and other technologies has made global transfers of personal information a common and essential component of daily life -- for both consumers and organizations. Yet, privacy protection varies dramatically from country to country. Some countries have comprehensive laws in place that regulate, among other things, cross border data transfers while others have little or no rules in place. For those countries that have privacy laws, both the standard of legal protection and the effectiveness of the enforcement of those laws vary significantly. This patchwork of laws provides illusory protections for consumers and reduces the choice and quality of products and services offered to them.

**The Solution.** The use of global or enterprise-wide privacy rules ("Corporate Privacy Rules") can correct the problems faced by consumers and organizations under the current international privacy regime. From a consumer perspective, Corporate Privacy Rules offer an effective method of protecting personal data no matter where the data are located throughout the world. They can ensure consumers' personal information is accorded a uniform level of protection, make local recourse mechanisms more widely available, and increase the choice and quality of products and services that can be offered to consumers. Moreover, Corporate Privacy Rules can be implemented, in most cases, within the context of existing legal frameworks, without the need to adopt new laws. Governments must be willing, however, to recognize the use of these rules as a legitimate and alternative means to safeguard cross border data transfers and establish an enforcement regime appropriate to their existing legal frameworks.

**Current Status.** For the past few years, the Coalition for Global Information Flows<sup>1</sup> has been working closely with the US Government to develop a regional privacy framework for the Asia Pacific Economic Cooperation ("APEC") Member Economies<sup>2</sup> that would permit the use of Corporate Privacy Rules to transfer personal information easily throughout the region. In November 2004, the Asia Pacific Economic Cooperation ("APEC") Member Economies approved a regional privacy framework that would permit the use of Corporate Privacy Rules to transfer personal information easily throughout the region. The APEC Privacy Framework is now in the process of

---

<sup>1</sup> The Coalition is comprised of a cross section of global businesses from the financial services, automobile, aerospace, consumer products, computer and computer software, communications, and electronic commerce sectors. The Coalition works to encourage responsible, global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the Coalition take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the Coalition. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

<sup>2</sup> The APEC Member Economies are: 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; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States; and Vietnam.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

being implemented within the Member Economies. In addition, Member Economies have agreed as part of the future work to: 1) develop a multilateral mechanism for sharing information among APEC Member Economies; 2) develop cooperative arrangements between privacy investigation and enforcement agencies of Member Economies; and 3) support the development and recognition of organizations' cross-border privacy codes across the APEC region.

*Next Steps.* For Corporate Privacy Rules to become a reality, governments will need to recognize their value and make them a policy priority. In particular, it will require creative, “out of the box” thinking about how to implement in their respective jurisdictions as well as a strong commitment to work closely with other governments to devise an approval process that will be acceptable to all. In many if not all of the jurisdictions, the proactive involvement of data protection/privacy authorities, consumer protection agencies, and other relevant agencies will be required.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

**Illustration of the Problem (See Appendix A for additional examples)**

*A US consumer purchases a computer from a US company and has trouble setting it up. Over a one week period, the consumer has to call the company's customer service support hotline at three different times of the day. Calls to the hotline between 9 am – 9 pm EST are handled by the US company, between 9 pm – 3 am EST by its Japanese affiliate, and between 3 am – 9 am EST by its Irish affiliate.<sup>3</sup>*

*Under current data protection rules, in order to provide this service and comply with the various national privacy laws,<sup>4</sup> the company must either obtain relevant personal information from the customer each time he calls (i.e. his name, contact information, information about his purchase to ensure that he is covered by the warranty and, require the customer to repeat the same information about his problem during each call with customer service or, to avoid such repetition, put into place four different contracts that will enable information to be shared among the affiliates. If the company opts for the latter approach, then the Irish affiliate must enter into a contract with the Japanese affiliate to transfer the data to it; the Irish affiliate must also enter into a contract with the US affiliate or the US affiliate must certify to the Safe Harbor. The Japanese entity must also enter into contracts with the Irish and the US affiliates. Even with such contracts in place, in addition to providing the customer a written notice at the time he initially provides his personal information to the company, the customer service representatives will still need to provide the customer with two or possibly three verbal privacy notices, before they can begin to address his problem.*

**Implications for Consumers And Business**

***Cumbersome Access Or Degraded Service For Consumers.*** The customer will be extremely frustrated that he must hear the privacy notice each time and, if there are no affiliate contracts in place, will likely be equally frustrated that he must provide his relevant data each time he calls customer service. He also will need to recount the content of all of his previous conversations with customer service because the affiliates will be unable to share with one another the information they collect from or advice they dispense to the customer. Moreover, the customer may not get an immediate response to his inquiry because, without access to a

---

<sup>3</sup> Since it is prohibitively expensive and extremely difficult to find qualified individuals to staff a customer services department in the United States 24 hours per day, the US company has opted to set up customer service centers in other parts of the world so that they can retain qualified individuals and provide 24 hours customer service.

<sup>4</sup> As of January 2006 forty countries have some form of data protection or privacy laws and at least ten other countries are considering adopting a privacy law. In addition to the local compliance obligations, many of these countries regulate cross border transfers of personal information, either explicitly prohibiting transfers to other countries unless certain conditions are met or imposing regulatory obligations on the organizations transferring the personal information. In most cases, organizations that want to transfer personal information legally have only two viable options available to them. They may either obtain the consent of the individual concerned or establish a contract with the entity that is receiving the data. Failure to adhere to these rules may result in civil and/or criminal penalties for the organization concerned.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

centralized database, the affiliate answering the customer's call must first obtain the customer's affirmative consent to request information from the affiliate from whom the purchase was made in order to verify, for example, the warranty information which it would need before it can provide an answer to the inquiry. This entire process could take hours or days to complete. For these reasons and those discussed below, some companies will forgo providing such support services entirely, thereby denying consumers access to such important services.

***Regulatory Burden Discourages Compliance and Provision of Goods and Services at Competitive Prices.*** For the company, the costs associated with establishing this type of customer services system is enormous. For example, if an organization with offices in 15 EU Member States, Japan, the US and Canada wishes to have a centralized customer data base to provide global customer services to its clients, the organization would be required to enter into 79 separate contracts among the corporate affiliates<sup>5</sup> and to have 18 different privacy notices. In addition, anytime there is an organizational change between the parties to the contract (e.g., a different affiliate is assigned responsibility for processing warranty data for a given affiliate or possibly on an enterprise-wide basis), new contracts will need to be negotiated. Or, if the organization relies on consent, then it must permit the individual to withdraw consent at anytime and keep track of those preferences. Because the cost of compliance is so administratively burdensome and so expensive, it may be easier simply to not provide 24 hour customer service.

***Disparities in Service Quality.*** The current system reduces business flexibility and inhibits businesses from managing their operations (e.g., controlling their costs) in an effective and efficient manner which, in turn, impacts the range and price of products and services offered to consumers. In particular, the existing arrangement discourages or impedes enterprise-wide initiatives in such areas as training, security, and procurement. Given the complexity and administrative burden of obtaining consent to transfer personal information, some organizations opt to implement such programs locally which makes it difficult to ensure the same level of standards are followed at the local level as well as achieve the same economies of scale that could be achieved if the program were operated on an enterprise-wide basis (e.g., negotiating supplier discounts on an enterprise-wide basis). So, in the customer service example cited above, the customer service representatives may not have the same level of troubleshooting expertise which will yield poorer support service for the customer.

---

<sup>5</sup> In certain situations, organizations will be unable to rely on the use of consent or contracts to make their international data transfers. For example, many banks and law firms function internationally through branches rather than through separate legal entities; therefore, contracts cannot be used when the same legal entity would be on both sides of the contract. Likewise, in certain jurisdictions consent is strongly disfavored particularly when it involves the transfer of employee data because there is a view that consent cannot be given "freely" within the context of the employment relationship or in exchange for goods or services. In addition if consent is the basis and a customer does not consent, then the organization may not be able to provide the services (i.e. a company cannot ship the goods if the individual will not permit the information to be disclosed to the affiliated entity that runs the fulfillment house where the goods are stored).

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

***Illusory Cross-Border Privacy Protection.*** Consumers are ill served because their personal information is not protected in a uniform and consistent manner. For example, if the above customer becomes a victim of identity theft as a result of a security breach by one of the affiliates or if an affiliate shares his personal information with a third parties against his wishes, the customer is likely to have a very difficult time resolving his problem, particularly since the affiliate from whom he purchased the computer is under no obligation to provide a local complaint resolution mechanism. As a result, the customer would have to overcome significant linguistic barriers as well as even larger legal barriers. First, the customer will have to determine who is at fault; however, even with superb computer forensics, it may be difficult to determine at precisely which point in the global network a hacker found entry. If it cannot be determined where in the system the hacking occurred or if the hack was from a completely different country and the information was collected in transmission between two affiliated entities, then it will be impossible to assign fault or responsibility for the security breach. Given that none of the affiliates will be responsible, each can avoid liability, thus leaving the consumer completely unprotected and with no viable recourse mechanism.

Second, the customer will need to determine that what law (or laws) applies, what his rights are with respect to the standard of protection in that jurisdiction, and who needs to be contacted to have the problem resolved. The answer to these questions may be very complex given the multi-jurisdictional nature of data flows; one or more sets of national rules will likely apply. It is entirely possible, given the jurisdictional differences in protections provided, that no privacy law has been violated. Consequently, the customer would have no recourse. The customer could appeal to the FTC for assistance but, unless the organization has demonstrated a pattern of abuse, the FTC is not likely to pursue redress for the customer. Alternatively, the customer might appeal to the local data protection authorities but often they are under staffed and under resourced and are not likely to take any action based on an issue raised by a US consumer.

**The Solution: Corporate Privacy Rules**

Allowing organizations to develop and implement Corporate Privacy Rules (“CPR”) govern their cross border data transfers of personal information can correct the problems faced by consumers and organizations under the current international privacy regime. In many jurisdictions, these rules can be enforced through existing legal frameworks. From a consumer perspective, CPR offer an effective method of protecting personal data no matter where the data are located throughout the world. They would provide consumers with consistent and enforceable rights even in jurisdictions with no privacy laws in place. In the event that there is a breach or unauthorized use of the customer’s personal information, the consumer will be able to file a complaint locally and in his native language and have the complaint addressed in an appropriate manner by the company with whom he has a relationship.

CPR also eliminate the need to determine which entity is at fault because a breach by one affiliate is treated the same as a breach by any other affiliate. The consumer’s rights and recourse are protected no matter where the breach occurs. Moreover, such rules will simplify

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

and reduce the cost of data privacy compliance for cross border transfers, thereby encouraging greater compliance. In particular, organizations will be able to implement a uniform privacy policies and practices on a regional or global basis without the administrative, legal, and organizational complexities of multiple contracts.

For example, suppose that one company had an affiliate in each of the 21 APEC Member Economies, each Member Economy had a cross border limitation, and the affiliates needed to share customer information across the region. If the organization had to rely on contracts in order to move customer data among the 21 APEC Member Economies, the organization would need 420 contracts among the affiliates (each affiliate would need to put in place a contract with the other 20 affiliates). If the organization were to use CPR, one set of rules would be required across all of the affiliates. From an organizational perspective having one set of CPR would make compliance much simpler and much less expensive and as a result much more likely to be widely adopted.

CPR are not a new concept; rather, they are an extension of an approach that has worked successfully in other areas for many years (*e.g.*, enterprise-wide policies in the field of financial reporting, and conflicts of interest). For these reasons, we believe that CPR could offer a new approach for consumers and organizations that will promote a broader culture of privacy.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

**APPENDIX A**

**ADDITIONAL EXAMPLES OF THE PROBLEM AND HOW CORPORATE PRIVACY RULES PROVIDES A VIABLE SOLUTION:**

The following are some additional examples that illustrate the illusive nature of the privacy protections afforded to consumers by the current international regime.

**1. No effective recourse mechanism**

a) *Scenario: A US consumer purchases a product over the Internet from a Malaysian company that is an affiliate of a US company. The individual voluntarily provides his information to the Malaysian company. The Malaysian company fails to properly secure the personal information of the individual and the US consumer becomes the victim of identity theft.*

b) Current Situation: Under the current privacy regime, the US consumer has few recourse alternatives. The US consumer (if he or she can speak Malay) could call and seek redress from the Malaysian company. If the Malaysian company fails to respond, the consumer could attempt to identify and file a complaint with the appropriate Malaysian authority. The consumer could call and seek redress from the US affiliate, but the US affiliate has no authority and possibly little influence over the Malaysian affiliate. Thus the US consumer effectively has no recourse.

c) Future Situation with CPR in Place: If the organization had adopted CPR, the consumer could see redress from the US company. Organizations that utilize CPR will agree to cooperate with consumers when an issue arises and help seek a solution even if the affiliate was not directly involved in the problem. In addition, the level of security and privacy that will be required across the organization will be consistent and, in particular, higher than required in those countries that have few legal or regulatory rules relating to privacy and data security. Thus the consumer will have a more effective recourse mechanism and the level of data security and privacy will rise across the organization.

**2. Privacy breach occurs but no privacy law is violated**

a) *Scenario: A US consumer is on vacation in Europe. The consumer asks the hotel where he is staying to make reservations for him at two other hotels in its chain in Asia and Latin America. At the consumer's request (e.g., with his consent), the European hotel transfers personal information about the consumer to the other hotels such as his name, address, and meal preferences which reveal his religion and credit card information. The hotel in Asia, located in a country that has a privacy law that contains very limited security obligations, fails to properly protect the information and the consumer becomes a victim of identity theft. In addition, the*

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

*hotel in Latin America, located in a country that has no privacy law in place, routinely sells its customer information to data brokers and the information is then used for other purposes.*

b) Current Situation: In this scenario, the consumer has no rights or guarantees that his personal information will be protected because he consented to the transfer. The European hotel did not violate European privacy laws because it transferred the information with the consent of the individual. It is not legally responsible for any misuse of that information by other hotels in its international chain. The Asian hotel is also not liable for any damages because it has minimal security safeguards in place that technically satisfy the local requirements (although they may fall far short of security requirements in jurisdictions with more rigorous standards). The hotel in Latin America is not liable because it is located in a country that has no privacy laws and therefore is also not limited to how it may use the data. Thus, the consumer has little protection and no effective recourse.

c) Future Situation with CPR in Place: If the organization had adopted CPR, the consumer could see redress from any of the three affiliates. Organizations that utilize CPR will agree to cooperate with consumers when an issue arises and help seek a solution even if the affiliate was not directly involved in the problem that arose. In addition, the level of security and privacy obligations that will be required across the organization will be consistent and, in particular, higher than required in those countries that have few legal or regulatory rules relating to privacy and data security. For example, the Latin American hotel would have to agree that despite the lack of laws in its country, it would not sell personal information of consumers absent consent. Similarly the Asian hotel would be required to adopt security standards which are consistent with the rest of the organization. Thus the consumer will have a more effective recourse mechanism and the level of data security and privacy protection will rise across the organization.

**3. Unable to determine who is at fault**

*a) Scenario: A US consumer purchases a computer product from a US company, using a credit card. The consumer's personal information will need to be shared with two different affiliates within the company: one for repair purposes and the other for customer services purposes. These affiliates are located outside the US. The company's US privacy policy discloses that customer information will be shared with affiliates of the organization for those purposes and the US company will safeguard the personal information that it processes in the US. It refers the consumer to the privacy policies of its affiliates for information about how those entities protect customer information. The consumer consents to this arrangement. If the consumer does not consent, she will not be able to obtain customer services nor have his product repaired. A hacker then breaks into the company's global computer system and steals the consumer's information.*

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

b) Current Situation: It may be very difficult for the consumer, even with superb computer forensics, to determine at precisely which point in the global network a hacker found entry. If it cannot be determined where in the system the hacking occurred or if the hack was from a completely different country, related to an affiliate, or the information was collected in transmission between two affiliated entities, then it will be impossible to assign fault or responsibility for the security breach. If the consumer approaches the US company, the US company can legitimately state that its systems were not hacked, rather it provided appropriate safeguards while the data was in its control, it obtained consent from the consumer before disclosing information to an affiliate and that the consumer needs to contact the affiliated entity to determine if there was a hack and to seek any redress.

c) Future Situation with CPR in Place: If the organization adopted CPR, the organization would not need to obtain the individual's consent in order to share the information with affiliates. Rather the organization would be free to operate its customer service and repair operations in the most efficient manner. The consumer would be entitled to go to the US company to see redress relating to the hacking incident. The US company would be obligated to address the hacking incident even if the hacking incident happened within an affiliate or in transit between the two affiliates. Thus the consumer would have effective redress with the company with which she established a business relationship.

#### **4. Diminished Services and Choice**

a) *Scenario*: A US consumer wants to travel to Argentina and calls a US travel agency. The US consumer is not interested in the travel agency's group travel packages and instead wants a customized itinerary for independent travel through Argentina. Because the US travel agency does not have all of the information requested by the consumer, it wishes to provide the consumer with the name and address of a travel agent from its affiliated travel agency in Argentina.

b) Current Situation: In order for the US travel agent to provide the business contact information of the Argentinean travel agent to the customer, the affiliated Argentinean travel agency would be required to give a notice to the individual Argentinean travel agent informing him or her that personal information is going to be collected and sent to the US so that a referral can be made, that US travel agents will have access to the information and that the information may be provided to customers in the US. In addition, it is likely that the individual travel agent in Argentina will have to consent to the provisions in the notice. Thus the US and Argentinean travel agencies would need to keep track of and ensure that each travel agent in Argentina receives a notice and consents to the collection, use and disclosure of his or her business contact information. In addition, if any one of the Argentinean travel agents later changes his or her mind and removed his or her consent, the US travel agent would have to be informed and the information relating to that travel agent would have to be removed from the database maintained by the US Travel Agency. As a result, the US and Argentinean travel agencies might decide that

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

it was too difficult to manage the notices and consents. Under those circumstances, the US travel agent could tell the consumer that no other information was available or provide the main telephone number and address of the Argentinean agency without providing the name of an individual travel agent. The travel agency might then lose the potential business if the consumer looks for another travel agency that can help locally. Alternatively, if the consumer decides to call the Argentinean agency directly, it might take several calls to identify the appropriate agent who can assist, an experience that will likely frustrate and annoy the consumer and undermine the overall business relationship with that consumer.

c) Future Situation with CPR in Place: If CPR were in place, the travel agency would be able to freely move the information between the US and the Argentinean travel agencies and provide that information to consumers. The consumers would be provided with quicker and better service.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

**APPENDIX B****CORPORATE PRIVACY RULES: IMPLEMENTATION OVERVIEW**

An organization should be able to elect to develop Corporate Privacy Rules ("CPR") that incorporate the principles established in the APEC Privacy Framework. Once the organization has developed its CPR, the rules then would be evaluated against the APEC Privacy Framework to assure that they are compliant. The process of assuring compliance with the APEC Privacy Framework may be accomplished in a number of ways, such as through attestations/self-declaration of compliance, review by designated third parties, or reviews by the relevant authority or agency. Defining this process is one aspect of the implementation work. To ensure credible and predictable enforcement, the compliance process will need to be consistent and uniform across participating APEC economies.

Once the compliance process has been completed successfully, the organization's rules would be regarded by all of the participating APEC Member Economies as satisfying the cross border data transfer requirements of each Member Economy without the need for further authorization or regulation. The organization would then be able to move data as required to meet its business needs among APEC Member Economies pursuant to its CPR. The organization would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice, access rights) if any in each of the Member Economies for the collection, use, and disclosure of personal data within the individual economies.

**I. APPROVAL OF CPR/VERIFICATION (OPTIONS A OR B)****A. An organization would self certify that its CPR complies with the APEC Privacy Framework.**

The self certification would involve an internal assessment of the organization's privacy practices to ensure that the organization's practices are in accord with the APEC Privacy Framework. The organization would be required to post its customer privacy policy online or make it publicly available. Privacy policies pertaining to the organization's workers would need to be provided to the workers and/or posted on the organization's Intranet and to the appropriate regulatory authorities in each Economy on request. In addition, the organization will need to conduct regular reviews of its practices to ensure compliance with the requirements and establish internal and external (third party) dispute settlement mechanisms.

As part of the process of implementing the CPR within its organization, the organization would also need to ensure that all of its affiliated entities with whom data will be shared apply the CPR to their handling of data within the APEC region. This could be accomplished in a

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

number of ways such as through intra-company agreements, intra-company corporate policies, revision of corporate bylaws, or unilateral declaration. The decision of how best to implement the CPR within an organization would be left up to individual organizations in order to accommodate their individual corporate structures and legal frameworks.

*OR*

**B. An organization would submit its CPR to a designated private or public entity for approval.<sup>6</sup>**

If a designated private or public entity reviews the CPR to ensure that it complies with the APEC Privacy Principles, its compliance review might involve some of the following:

- verification that there is an online privacy policy posted that covers the APEC Privacy Principles;
- completion of a privacy assessment questionnaire;
- monitoring and review by a trusted organization; or
- designation of a dispute resolution mechanism.

A hybrid approach may include the development of an approval or verification process by public sector entities, which would be carried out by authorized private sector entities. Such a process could include guidance in the forms of checklists or other documents that set forth essential code aspects or factors to satisfy the verification process. While there is a desire to obtain consistent outcomes in the verification process, some flexibility must be maintained to allow for variances in business models, customer bases, sectors and legal frameworks.

## **II. PUBLIC DECLARATION (OPTIONS)**

**A. An organization would make a public declaration that it will protect personal data that it transfers from one jurisdiction to another in accordance with its approved CPR.**

The declaration could be included in the organization's privacy policy or some other public statement that is posted to its website (or in the case of workers, to its Intranet). The organization would need to designate or indicate the APEC Economy in which it is certifying its Code. There should be a logical connection between the designated economy and the

---

<sup>6</sup> If a nonprofit organization carried out these functions, the regulatory body then would need to give priority to referrals of non-compliance with guidelines that govern the private organizations. If these private organizations fail to carry out their responsibilities (e.g., they approve Codes without undertaking the proper due diligence), their conduct would be actionable, in the case of the US, under the FTC's unfair and deceptive trade practices authority or enforcement authority of other regulatory bodies.

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

organization's operations (e.g., the APEC Economy selected might be the jurisdiction in which it has its center of activity or in which it is headquartered).

**OR**

**B. An organization would make a public declaration that it will protect personal data that it transfers from one jurisdiction to another in accordance with its CPR by registering its commitment with a designated private or public entity.**

The declarations/registrations would be submitted by the organization to a private or public body and would then be available online for public inspection.

Once an organization makes a public declaration, then the organization's CPR would be regarded by all of the other APEC Member Economies as satisfying the "cross border" data transfer requirements of each Member Economy without the need for further authorization or regulation. The organization could then move data as needed among APEC Member Economies pursuant to its CPR. The organization would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice, access rights) if any in each of the Member Economies for the collection, use, and disclosure of personal data within the individual economies.

### **III. Complaint Handling**

Those organizations that elect to participate in a CPR process will provide information on their complaint handling procedure in either their privacy policy or another document that is made available to the individual concerned. This information will detail the manner in which and to whom complaints should be addressed; the existence of any third party dispute resolution mechanisms, and the regulatory authority or agency that will receive complaints from individuals once all other dispute resolution mechanisms have been tried.

Complaints about any handling of personal information would be addressed first through the organization's internal complaint handling process. If the complaint cannot be resolved internally, then the organization is strongly encouraged to have an independent dispute resolution mechanism in place that can be used.

Possible third party dispute resolution programs in the United States include those run by organizations such as BBBOnline, TRUSTe, AICPA WebTrust, and the Direct Marketing Association. In addition, outside arbitration and mediation service such as JAMS or the American Arbitration Association could also be used. In countries with an independent data protection authority the appropriate DPA could provide the dispute resolution mechanism. In other countries, such as Japan, other private dispute resolutions mechanisms are available.

The dispute resolution mechanism, to be effective, must be independent, readily available, and affordable. Damages, penalties, and/or sanctions may be awarded where the

**Coalition For Global Information Flows  
Comments On The Development And Implementation Of  
Cross-Border Privacy Rules In The Asia  
Pacific Cooperation Group (APEC)**

applicable law or private sector initiatives so provide. The organizations should also be obligated to remedy problems arising out of its failure to comply with its Code; and persistent failures of the organization to comply with rulings could result in the loss of their Code certification.

If the dispute still cannot be resolved, then the matter can be referred to the appropriate governmental or regulatory body responsible for privacy protection (such as the FTC, FCC, OCC or other appropriate body in the US) or, when such an agency does not exist, the public prosecutor in that economy. The governmental or regulatory body would then work with the organization and/or third party certification body (if applicable) to resolve the dispute. If the organization refuses to comply with the decision of the regulatory body, then it would also be subject to penalties and sanctions.

**IV. CROSS BORDER COOPERATION**

All of the APEC data protection or regulatory bodies would need to agree to cooperate in the event of cross border disputes or breaches. Such an agreement could take the form similar to a mutual recognition or cooperation agreement.