

THE AMERICAS

CROSS-BORDER ISSUES

How does 'privacy' translate abroad?

A new initiative will govern international transfers of information.

By Martin Abrams
SPECIAL TO THE NATIONAL LAW JOURNAL

FOR EVERY COMPANY in the Americas of any size, cross-border data transfers are a way of life. Offices in Lima, Peru, access customer information stored in Toronto. A distribution center in Cincinnati processes accounts payable in Costa Rica and Mexico. A clinical research team in New Jersey shares data with teammates in 12 countries outside the United States. A clinic in Vancouver, British Columbia, has systems serviced in Rochester, N.Y. Today, data are processed anywhere, by everyone, and at anytime—they are constantly moving.

Much of this information pertains to people, which means it is sensitive from both a privacy and security standpoint. Privacy and security require the information to be under control as it moves and sits, and control requires governance. This article will focus on governance as it exists today in the Americas and governance as it probably will exist in the very near future based on a framework being developed by the Asia Pacific Economic Cooperation (APEC) group of Pacific Rim nations.

The implementation structure for the framework is being built out in 2008 as part of the APEC year in Peru (member states take turns hosting the annual APEC summit). Nine privacy pathfinder projects were approved during the 2007 APEC year in Australia. Those pathfinders are being explored during two APEC privacy workshops in Peru in 2008—one that was held in February and another to be held in the fall. This process will establish the governance structure for the next decade.

Canada and the United States already have governance structures for cross-border data transfers. The Canadian law is explicit, while U.S. protections are inferred from other laws. The following describes the protections that exist today in the Americas:

Martin Abrams is executive director of the Center for Information Policy Leadership at Hunton & Williams. The center is a global privacy and information security think tank located in Washington.

Canada has omnibus privacy laws that govern both the public and private sectors. The laws are maintained at both the federal and provincial level. Canada's federal private-sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, available at www.canlii.org/ca/sta/p-8.6/, is considered by many experts to be the most progressive legislation on international data transfers in the world. The law requires an organization to comply with a set of standard data-protection principles. Canadian law makes no distinction between information processed by the organization and by a vendor for the organization. The law makes no distinction between processing in Canada and processing Canadian resident data outside Canada.

Responsible for vendors

Either way, the Canadian organization that collects information from or about the individual is accountable for the protection of that information. If a Canadian company outsources a process to a company anywhere else in the world, the Canadian company remains accountable for how that vendor manages and protects the information. If a vendor in Mexico is processing the information for a Canadian firm covered by the act (such as a bank) and has a data breach that harms Canadian individuals, the Canadian authorities will pursue that Canadian firm for redress.

Quebec, Alberta and British Columbia have provincial private sector laws that are equivalent to the federal law. Ontario does not have an omnibus private sector act, but does have a law covering health care that is equivalent for health-related privacy.

None of Canada's privacy commissioners have the power to levy fines directly. Instead, the commissioners' roles are those of ombudsmen. The PIPEDA is currently up for review, however, and may be amended to give the federal commissioner more authority.

There is a complicating factor under Canadian law: Canadian privacy officials and many Canadian consumers mistrust national security and law enforcement officials in the United States. Power granted to U.S. officials under the USA Patriot Act and other acts to subpoena data accessible from the

United States has outraged Canadians, even though Canadian officials hold similar authority. British Columbia has passed legislation that prohibits the outsourcing of public-sector processes to vendors who might have the information accessed from the United States.

Other provinces are considering similar laws, and there have been threats of expanding the requirement to the private sector.

These issues have been a topic for negotiations among Mexico, Canada and the United States to expand trade among the three neighbors.

Outsourcers have a duty to protect their clients' privacy.

The U.S. approach

There are no laws that would prohibit U.S. companies from processing information outside the United States. However, existing laws are being interpreted to require that data collected from or on individuals in the United States must be protected no matter where the information is processed or by whom.

This concept was articulated clearly in a May 7, 2004, letter from then-Federal Trade Commission Chairman Timothy Muris to U.S. Representative Edward Markey, D-Mass.: "A company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws," Muris wrote. "Simply because a company chooses to outsource some of its data processing to a domestic or offshore service provider does not allow that company to escape liability for any failure to safeguard the information adequately." Letter from Timothy J. Muris, Chairman, Federal Trade Commission, to U.S. Representative Edward Markey (May 2, 2004) (on file with author).

The primary law that Muris was referring to was the Safeguards Rule contained in the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA). The act requires financial services companies to provide physical, technical and administrative safeguards for personal financial

information. While GLBA covers only financial services companies, the Federal Trade Commission (FTC) has asserted that as a matter of fairness, organizations must safeguard information pertaining to individuals under their care.

Therefore, U.S. companies will be held accountable if information they export or make accessible outside the United States is lost, stolen or misused. While contracts may be used to specify outsourcer responsibilities, the totality of the process will be examined by the FTC. If the outsourcer did not conduct due diligence to determine the vendor's willingness and capacity to adhere to the contract, then the outsourcer may well find itself signing a consent decree with the FTC.

While the FTC lacks authority over banks and many other financial services companies, those institutions are covered by safeguard regulations very similar to the FTC's. Trade groups within financial services, such as the Banking Industry Technology Secretariat, have been developing standards for security in an outsourcing environment.

Latin America is becoming a data destination.

Mexico and Costa Rica have become prime outsourcing locations for processes originating in North America. Brazil has become a destination for information, and Chile has targeted electronic commerce as an engine for growth. Argentina has a privacy law that has been found adequate by Europe, but enforcement of the law is almost nonexistent. Chile, Panama and Uruguay have privacy laws to some extent, but don't seem to create a risk for parties transferring data.

Mexico has been debating privacy legislation for years, but seems no closer to passing new laws. Essentially, data transfer governance requirements from most Latin American countries are not a current compliance issue.

Focus on accountability

Accountability is the key theme for cross-border data transfers from North America. That key concept of accountability most likely will be the evolving standard for cross-border data transfer governance. Accountability is part of the Canadian law PIPEDA and is inferred by the Safeguards Rule and its broader application as a fairness standard by the FTC.

The concept of accountability was first articulated by the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines of 1980, which included Canada, Mexico and the United States as signatories. See www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html. However, the OECD principle has not been developed into a governing structure for data transfers.

APEC has begun to fill the vacuum. Its key motivator is economic growth in the region. APEC is

relevant to the Americas because it includes Chile, Peru, Mexico, the United States and Canada.

Steering group formed

APEC created the Electronic Commerce Steering Group in 1998, and that group created a subgroup to consider privacy issues. APEC includes 21 economies with varying levels of privacy law and sophistication. Canada, Hong Kong, Australia and New Zealand have data-protection laws and independent privacy commissioners; Japan and South Korea have privacy laws with unique structure; the United States has its own, very special privacy mosaic.

Most of the other APEC countries lack privacy laws and have very different privacy cultures. The APEC economies determined that this mixture of privacy approaches might eventually prove an impediment to electronic commerce-led economic growth. In 2003, the data privacy subgroup began developing a framework for privacy so that concerns about privacy would not inhibit the economic growth that would come from electronic commerce.

The APEC Privacy Framework, approved in 2004, was based on the well established OECD guidelines. Asia-Pacific Economic Cooperation, APEC Privacy Framework, 2004; available at www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html. However, the accountability principle was strengthened and established as the primary governance structure for cross-border data transfers.

The APEC accountability principle states: "A personal information controller should be accountable for complying with the measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." *Id.* at 19.

The APEC process references corporate cross-border privacy rules. A set of cross-border privacy rules is an approved set of policies that match the APEC privacy principles and that a company promises to put into effect to govern its protection of personally identifiable information.

As mentioned above, the rules must be compliant with the APEC principles, and the company must agree that it will follow national privacy laws that exist where the information is collected. The rules must be approved by an accountability agent, and a national authority must submit the name of the approved entity to the APEC Secretariat to be posted to a Web site.

Once a company's cross-border rules are approved by one economy, they must be recognized by all other participating economies. For example, a U.S. company approved in the United States would be free to collect information in Thailand and process it in Hong Kong if all three

economies are participating.

Each APEC economy is free to create the structure for approval and oversight that best matches its legal system and privacy culture. Many APEC economies will choose to use nongovernmental entities as accountability agents, such as trademark agencies.

Other economies will use existing data-protection authorities as accountability agents. No matter which structure is adopted, a government authority will have responsibility for enforcement.

New privacy rules could be in effect sometime next year.

Pathfinder projects

While each economy may have its own structure for approvals, they must all use similar standards. This is important because an approval of a set of cross-border privacy rules by one economy must be respected by all other participating economies. To build out these standards, APEC approved a set of pathfinder projects. Thirteen economies are participating in the pathfinder, including all of the economies in the Americas.

The purpose of the pathfinder projects is to develop the documents and processes necessary for approval, recognition and processing of consumer disputes. For example, one pathfinder project is exploring what documents are necessary for privacy enforcement agencies in different economies to hand off disputes to other economies. see http://aimp.apec.org/Documents/2007/ECSG/SEM2/07_ecsg_sem2_003.doc. This Pathfinder Project Nine is a test bed for the standards and processes.

Both Mexico and the United States are participating in the project and have companies that have agreed to participate in the tests. The participating companies will test the documents and processes to see whether they are usable to create a governance means for cross-border data transfers. The regulators will use dummy complaints against the companies to see if the redress program works.

The pathfinder projects should be completed in early 2009. It can be expected that a number of companies will begin to use APEC cross-border privacy rules in the latter part of 2009.

Organizational accountability is the emerging governance structure for cross-border data transfers. To be accountable, organizations will have to develop internal policies that are compliant with traditional privacy principles and have mechanisms to ensure that these principles are enforced both within the organization and with its vendors. Accountability structures will be mandatory for any organization that distributes work where it may most effectively be performed. **NLJ**