



## Why are more companies joining the U.S. - EU Safe Harbor privacy framework?

By Brian Hengesbaugh, Michael Mensik, and Amy de La Lama of Baker & McKenzie LLP

*This story originated as a Baker & McKenzie LLP North America Global Privacy Client Alert and is republished here with permission*

The U.S. Department of Commerce (U.S. DOC) recently held its 2009 International Conference on Cross Border Data Flows & Privacy in Washington, DC. The U.S. DOC announced at the conference that an increasing number of companies are choosing to self-certify compliance with the U.S.-EU Safe Harbor Privacy Framework (Safe Harbor). Every month, approximately 50 companies file initial self-certifications to the Safe Harbor, and approximately 150 companies submit annual re-certifications. More than 50 percent of the companies in the Safe Harbor have joined during the past two years. At present, there are more than 2,100 companies included on the U.S. DOC's Safe Harbor list. Placed in context, this means



Brian Hengesbaugh



Michael Mensik



Amy de La Lama

that more companies join Safe Harbor in a single month than the total number of companies that have obtained approval for binding corporate rules to date (as discussed later, such binding corporate rules are another key approach to cross-border data transfers).

*See, U.S. - EU Safe Harbor, page 4*



Nancy A. Cohen

## AICPA and CICA update Generally Accepted Privacy Principles

By Nancy A. Cohen, CPA.CITP, CIPP, and Nicholas F. Cheung, CA, CIPP/CA

Establishing an annual privacy risk assessment process to identify new or changed risks to personal information is a key enhancement to Generally Accepted Privacy Principles (GAPP). GAPP is an internationally recognized privacy framework developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

"An annual risk assessment is critical to understanding the privacy risks within an organization," said Everett C. Johnson, CPA, chair of the AICPA/CICA Privacy Task Force and a past international president of ISACA. "Once those risks are identified and assessed, the organization can then take the



Nicholas F. Cheung

## This Month

The year ahead: privacy predictions 2010.....	3
Managing global data privacy.....	14
Privacy and pandemic planning.....	15
The Lisbon Treaty and data protection.....	17
New international privacy principles for law enforcement and security.....	18
FTC privacy roundtable signals policy shift.....	20
Global Privacy Dispatches.....	26
Calendar of events.....	29
Privacy news.....	29
Surveilled.....	30
10 privacy resolutions.....	34

*See, GAPP update, page 10*

# PRIVACY PREDICTIONS -2010-

## Data protection in France 2010

This year the odds are that the French data protection environment will likely see a strengthening of legal requirements by the introduction of an obligation to provide data breach notifications and another obligation to appoint a data protection official. At the same time, on the DPA side we will see more and more onsite investigations.

One can also foresee the growth of the privacy profession and the growth of the AFCDP, the French Association of Data Protection Correspondents.

—*Pascale Gelly, Partner, Cabinet Gelly; Member, Board of Directors of AFCDP*

## Privacy and data protection in Israel, 2010

LITA will submit legislative reform to Knesset, tightening enforcement, increasing accountability, and reducing bureaucratic burdens. The Supreme Court will rule on major constitutional challenge to Communications Data Act, asserting disproportionate effect on privacy. Privacy professionals will descend on Jerusalem October 27-28 to celebrate IAPP annual soccer match (and the 32nd annual Conference of Privacy and Data Protection Commissioners).

—*Omer Tene, Israeli Legal Consultant, Associate Professor, College of Management School of Law, Israel*

## GAPP update

*continued from page 1*

appropriate steps to address those risks. We've updated the criteria of our privacy principles to mitigate the risks to personal information."

*Generally Accepted Privacy Principles*, last updated in 2006, are designed to help an organization's management develop a program that addresses their privacy obligations and risks and to assist them with assessing their existing privacy program. It is also the basis for a privacy audit that can be performed by a Certified Public Accountant or Chartered Accountant. GAPP incorporates concepts from local, national, and international laws, regulations, guidelines, and other bodies of knowledge on privacy into a single privacy objective. This objective is supported by 10 privacy principles:

**1. Management** – The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

**2. Notice** – The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

**3. Choice and consent** – The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

**4. Collection** – The entity collects personal information only for the purposes identified in the notice.

**5. Use, retention, and disposal** – The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations, and thereafter appropriately disposes of such information.

*"Each principle is supported by objective, measurable criteria for handling personal information throughout an organization."*

**6. Access** – The entity provides individuals with access to their personal information for review and update.

**7. Disclosure to third parties** – The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

**8. Security for privacy** – The entity protects personal information against unauthorized access (both physical and logical).

**9. Quality** – The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

**10. Monitoring and enforcement** – The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Each principle is supported by objective, measurable criteria for handling personal information throughout an organization. Together, this set of privacy principles and related criteria are useful to those who:

- oversee and monitor privacy and security programs;
- implement and manage privacy and security;
- oversee and manage risks and compliance;

*See, GAPP update, page 12*

## The IAPP Welcomes our Newest Corporate Members



**Jordan Lawrence™**



An MLF Financial Group Company



Looking at LIFE in a new light™

A Maple Life Financial/Cantor Fitzgerald Company



Adding value to LIFE investments™



### GAPP update

*continued from page 10*

- assess compliance and audit privacy and security programs; regulate privacy.

The changes, which include eight new criteria (now more than 70 in total) and the modification of two others, were the result of deliberations and consideration given to comments received from the public in response to the exposure draft that was released in March 2009.

“Safeguarding personal information is one of the most challenging responsibilities an organization has, whether it’s information pertaining to employees or customers,” said Johnson. “We’ve updated the criteria of our privacy principles to minimize the risks to personal information. We have enhanced the guidance on security, breach response, and employee-related matters, along with disposal and destruction of personal information.”

The following is a summary of the new criteria:

#### **Personal Information Identification and Classification (1.2.3)**

– The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity’s privacy and related security policies and procedures.

This may include having an information-classification process that identifies and classifies information into categories such as business confidential, personal information, business general, and public.

#### **Risk Assessment (1.2.4)**

– A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and develop and update responses to such risks.

Risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as e-mailing unprotected sensitive information). Ideally, the

privacy risk assessment should be integrated with the security risk assessment and be a part of the entity’s overall enterprise risk management program. The AICPA and CICA have developed a Privacy Risk Assessment Tool that organizations may find useful.

#### **Privacy Incident and Breach (1.2.7)**

– A privacy incident and breach management program has been documented and implemented. It includes, but is not limited to, the following:

- procedures for the identification, management, and resolution of privacy incidents and breaches;
- defined responsibilities;
- a process to identify incident severity and determine required actions and escalation procedures;
- a process for complying with breach laws and regulations, including stakeholders breach notification, if required;
- an accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate;
- a process for periodic review of actual incidents to identify necessary program updates;
- periodic testing or walkthrough process and associated program remediation as needed.

#### **Privacy Awareness and Training**

**(1.2.10)** – A privacy awareness program about the entity’s privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.

“Ensuring that employees are educated about privacy will help prevent privacy breaches, improve customer service, and demonstrate the organization’s commitment to sound business practices,” explains Donald Sheehy, CA-CISA, CIPP/C, associate partner with Deloitte

*“Portable devices such as laptops and memory sticks provide convenience to employees, but appropriate measures must be put in place to properly secure them and the data they contain.”*

(Canada) and a Canadian member of the AICPA/CICA Privacy Task Force.

**Information Developed about Individuals (4.2.4)** – Individuals are informed if the entity develops or acquires additional information about them for its use. Such information may be obtained or developed from third-party sources, browsing, and credit/purchasing history.

**Disposal, Destruction and Redaction of Personal Information (5.2.3)** – Personal information no longer retained is made anonymous, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access. This can include the removal or redaction of specified personal information about an individual, such as removing credit card numbers after the transaction is complete and using companies that provide secure destruction services.

**Personal Information on Portable Media (8.2.6)** – Personal information stored on portable media or devices is protected from unauthorized access.

Policies and procedures prohibit the storage of personal information on portable media or devices unless a business need exists and such storage is approved by management. Such information is encrypted, password protected, physically protected, and subject to the entity’s access, retention, and destruction policies. Upon termination of

employees or contractors, procedures provide for the return or destruction of portable media and devices used to access and store personal information, and printed and other copies of such information.

“Portable devices such as laptops and memory sticks provide convenience to employees, but appropriate measures must be put in place to properly secure them and the data they contain,” related Sheehy. “We must stay abreast of technological advances to ensure that proper measures are put into place to defend against any new threats.”

**Ongoing Monitoring (10.2.5)** – Ongoing procedures are performed for monitoring the effectiveness of controls over personal information based on a risk assessment and for taking timely corrective actions where necessary. An example of a control would be reviewing employee files to seek evidence of course training in compliance with policies that require all employees take initial privacy training within 30 days of employment.

Other changes to GAPP include restricting the use of personal information in process and systems testing, references to ISO 27002, and revised language for auditors to use when preparing reports on a privacy audit.

Several organizations worked in conjunction with the AICPA and CICA on GAPP, including ISACA and the Institute of Internal Auditors. Copies of GAPP, along with additional privacy resources, are available at [www.aicpa.org/privacy](http://www.aicpa.org/privacy) and [www.cica.ca/privacy](http://www.cica.ca/privacy).

*Nancy A. Cohen, CPA.CITP, CIPP, (ncohen@aicpa.org) is Senior Technical Manager - Quality Control, Research & Development for the American Institute of Certified Public Accountants.*

*Nicholas F. Cheung, CA, CIPP/C, (nicholas.cheung@cica.ca) is a principal with the Canadian Institute of Chartered Accountants.*

*Both Nancy and Nicholas are members of the AICPA/CICA Privacy Task Force.*

## Privacy Classifieds

*The Privacy Advisor* is an excellent resource for privacy professionals researching career opportunities. For more information on a specific position, or to view all the listings, visit the IAPP’s Web site, [www.privacyassociation.org](http://www.privacyassociation.org).

### PRIVACY RESEARCH ALLIANCE COORDINATOR

Nymity  
Toronto, ON

### PRIVACY RESEARCH SPECIALIST

Nymity  
Toronto, ON

### VULNERABILITY MANAGEMENT AND SECURITY COMPLIANCE RISK ASSESSOR

Convergys  
Cincinnati, OH

### PRIVACY PROJECT MANAGER

Genentech  
South San Francisco, CA

### PRIVACY RESEARCH LAWYER

Nymity  
Toronto, ON

### MANAGER/SENIOR MANAGER U.S. CONSUMER AND SMALL BUSINESS PRIVACY

American Express  
New York, NY

### SENIOR MANAGER, INFORMATION SYSTEMS SECURITY

Convergys  
Dallas, TX

### PRIVACY COMPLIANCE SPECIALIST

U.S. Department of Homeland Security,  
Privacy Office  
Rosslyn, VA

### PRIVACY DIRECTOR

Blue Shield of California  
San Francisco, CA

### PRIVACY ACT CONSULTANT

RGS Associates, Washington Navy Yard  
Washington, DC