



## 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*

## THE PRIVACY ADVISOR

### Editor

Kirk J. Nahra, CIPP, Wiley Rein LLP  
knahra@wileyrein.com  
+202.719.7335

### Publications Director

Tracey Bentley  
tracey@privacyassociation.org  
+207.351.1500

*The Privacy Advisor* (ISSN: 1532-1509) is published by the International Association of Privacy Professionals and distributed only to IAPP members.

### ADVISORY BOARD

*Miranda Alfonso-Williams*, CIPP, CIPP/IT, Global Privacy Leader, MDx GE Healthcare

*Nathan Brooks*, CIPP

*Kim Bustin*, CIPP/C, President, Bustin Consulting Limited

*Debra Farber*, CIPP, CIPP/G, Privacy Officer, The Advisory Board Company

*Benjamin Farrar*, CIPP, Manager, Privacy Team, Quality & RM, Ethics & Compliance, Ernst & Young LLP

*Steven B. Heymann*, CIPP, VP, Compliance and Information Practices, Experian

*Michael Kearney*, Student/Research Assistant, William & Mary School of Law

*Jim Keese*, CIPP, Global Privacy Officer, VP Records & Information Mgmt, The Western Union Company

*Stephen Meltzer*, CIPP, Privacy and Corporate Counsel, Meltzer Law Offices

*David Morgan*, CIPP, CIPP/C, Privacy Officer-Secondary Uses, Newfoundland and Labrador Centre for Health Information

*Dan Ruch*, Privacy and Data Protection Consultant, KPMG

*Luis Salazar*, CIPP, Partner, Infante, Zumpano, Hudson & Miloch, LLC

*Heidi Salow*, CIPP, Of Counsel, DLA Piper

*Julie Sinor*, CIPP, Information Management Consultant, PricewaterhouseCoopers, LLP

*Eija Warma*, Associate Attorney, Castren & Snellman Attorneys Ltd

*Frances Wiet*, CIPP, Chief Privacy Officer, Hewitt Associates LLC

### To Join the IAPP, call:

+800.266.6501

### Advertising and Sales, call:

+800.266.6501

### Postmaster

Send address changes to:

IAPP  
170 Cider Hill Road  
York, Maine 03909

### Subscription Price

*The Privacy Advisor* is an IAPP member benefit. Nonmember subscriptions are available at \$199 per year.

### Requests to Reprint

Tracey Bentley  
tracey@privacyassociation.org

Copyright 2010 by the International Association of Privacy Professionals. All rights reserved. Facsimile reproduction, including photocopy or xerographic reproduction, is strictly prohibited under copyright laws.

## Notes From the Executive Director

### Looking forward and back

Rewind 10 years. Social networking involved the spoken word, smart phones were less intelligent, and nobody “noticed” when there was a security breach. And a handful of people gathered around the idea that the emerging role of privacy within organizations needed a bit more networking and collaborative education. The IAPP was born.



In the months ahead we will look back over the 10 remarkable years that have shaped our profession, so far. To kick off the yearlong anniversary celebration, we’ll come together in Washington, DC and at telecast locations around the world to share memories and to look ahead to future decades with the release of our report *The Road Ahead: The Next-Generation Privacy Professional*. We hope you will join us for what is bound to be a memorable milestone.

Not everything is worth remembering, but in today’s world of hyper-connectivity, massive data flows, and cheap storage, we can relive faded memories at the click of a mouse. The affect of this near-perfect memory on human processes such as forgiving and healing has been an area of study for Viktor Mayer-Schönberger, an information governance scholar who says the act of ‘forgetting’ has a social value that could be in jeopardy. Mayer-Schönberger is the author of *Delete: The Virtue of Forgetting in the Digital Age*. He will join us at the upcoming Global Privacy Summit in April to discuss this and the concept of ‘data expiration dates.’

Also joining us at Summit will be Dan Ariely. Ariely is a behavioral economist and the author of *Predictably Irrational: The Hidden Forces That Shape Our Decisions*. Why consumers do what they do with their data is a question at the very heart of our work in the privacy field. Ariely will shed light on this and other human behaviors that relate to privacy and data protection. We look forward to seeing you there.

We also look forward in this issue of the *Privacy Advisor*, with experts’ forecasts for the year ahead. We hope you enjoy the issue and hope to see you at upcoming events.

J. Trevor Hughes, CIPP  
Executive Director, IAPP

## THE YEAR AHEAD:

# PRIVACY PREDICTIONS -2010-

At the end of each year, the Privacy Advisor polls professionals worldwide to find out what they see in the year ahead for privacy and data protection. In this first issue of 2010, we present their forecasts. We begin with that of Canadian Privacy Commissioner Jennifer Stoddart. Commissioner Stoddart is entering her seventh and final year as Privacy Commissioner of Canada. In 2009 her office made worldwide waves with its unprecedented investigation into the privacy policies and practices of social networking giant Facebook. Her office will continue to monitor the privacy practices of social networking sites in the year ahead, in addition to other areas she anticipates will command attention.

Here is Commissioner Stoddart's forecast. See more 2010 predictions throughout the newsletter.

## PREDICTIONS for privacy and data protection in Canada, 2010

In 2010, Canada's privacy landscape will be painted in many of the same hues and textures familiar to Americans and others around the globe—the disquieting shadows of ever-tightening security measures, the striking, often puzzling, palette of bold new consumer technologies. And, dawning over the horizon, are unsettling new ways to extract even the most personal of information from the genetic material of human beings.

Focused as we are on helping Canadians protect the integrity of their identities, my office will continue to advance our longstanding efforts to hold social networking sites accountable for the personal information entrusted to them by Canadians. While British Columbia hosts the world at the 21st Winter Olympics, we will be monitoring the privacy implications arising from a mounting array of national security initiatives. Biometrics and genetic technologies pose other privacy challenges of concern to us. And emerging information technologies, such as cloud computing and the tracking, profiling, and targeting of consumers by business, will become major focuses of interest as the year unfolds.

The need for consistent and enforceable global privacy standards has never been more important. We will continue to participate in the international dialogue, which will continue to intensify.

—Jennifer Stoddart  
Privacy Commissioner of Canada



# iapp

international association of privacy professionals

170 Cider Hill Road  
York, ME 03909  
Phone: +800.266.6501 or +207.351.1500  
Fax: +207.351.1501  
Email: information@privacyassociation.org

The Privacy Advisor is the official newsletter of the International Association of Privacy Professionals. All active association members automatically receive a subscription to The Privacy Advisor as a membership benefit. For details about joining IAPP, please use the above contact information.

### BOARD OF DIRECTORS

#### President

**Nuala O'Connor Kelly**, CIPP, CIPP/G, Chief Privacy Leader & Senior Counsel, Information Governance, General Electric Company, Washington, DC

#### Vice President

**Bojana Bellamy**, LL.M., Director of Data Privacy, Accenture, London, UK

#### Treasurer

**Jeff Green**, CIPP/C, VP Global Compliance & Chief Privacy Officer, RBC, Toronto, ON, Canada

#### Secretary

**Jane C. Horvath**, CIPP, CIPP/G, Senior Global Privacy Counsel, Google Inc., Washington, DC

#### Past President

**Jonathan D. Avila**, CIPP, Vice President - Counsel, Chief Privacy Officer, The Walt Disney Company, Burbank, CA

#### Executive Director, IAPP

**J. Trevor Hughes**, CIPP, York, ME

*Allen Brandt*, CIPP, Corporate Counsel, Chief Privacy Official, Graduate Management, Admissions Council, McLean, VA

*Agnes Bundy Scanlan*, Esq., CIPP, Chief Regulatory Officer, TD Bank, Boston, MA

*Malcolm Crompton*, CIPP, Managing Director, Information Integrity Solutions Pty/Ltd, Chippendale, Australia

*Stan Crosley*, Esq., CIPP, Partner, Co-Director, Indiana U. Center for Strategic Health Information Provisioning, Indianapolis, IN

*Dean Forbes*, Senior Director Global Privacy, Schering-Plough Corporation, Kenilworth, NJ

*D. Reed Freeman, Jr.*, CIPP, Partner, Morrison & Foerster, LLP, Washington, DC

*Sandra R. Hughes*, CIPP, Global Ethics, Compliance and Privacy Executive, The Procter & Gamble Company, Cincinnati, OH

*Alexander W. Joel*, CIPP, CIPP/G, Civil Liberties Protection Officer, Office of the Director of National Intelligence, Bethesda, MD

*Brendon Lynch*, CIPP, Senior Director, Privacy Strategy, Microsoft Corporation, Redmond, WA

*Lisa Sotto*, Esq., Partner, Hunton & Williams LLP, New York, NY

*Scott Taylor*, Chief Privacy Officer, Hewlett-Packard, Palo Alto, CA

*Florian Thoma*, Chief Data Protection Officer, Siemens, Munich, Germany

*Richard Thomas CBE LLD*, Centre for Information Policy Leadership, Hunton & Williams LLP, Surrey, UK

*Brian Tretick*, CIPP, Executive Director, Advisory Services, Ernst & Young, McLean, VA

#### Ex Officio Board Member

*Kirk J. Nahra*, CIPP, Partner, Wiley Rein LLP, Washington, DC



**U.S. - EU Safe Harbor***continued from page 1*

Why are increasing numbers of companies joining the Safe Harbor? What factors cause companies to choose Safe Harbor over other approaches to addressing cross-border data transfer restrictions? This article explores some of the drivers for an increasing number of “Safe Harborites,” and identifies key differences between Safe Harbor and the alternative approaches. It also discusses special issues related to outsourcing service providers, recent enforcement actions, and trends related to global privacy compliance.

**1. What is the Safe Harbor and how does it work?**

The Safe Harbor is one approach U.S. companies can adopt to address the cross-border data transfer restrictions under the European Commission’s 1995 Data Protection Directive (95/46/EC) (Directive). Specifically, the Directive prohibits the transfer of personally identifiable information about individuals located in the European Union (EU Personal Data) to the United States or other locations outside the European Economic Area, unless the data recipient is subject to a law or other binding scheme that provides “adequate protection” for such EU Personal Data (Data Transfer Restriction), or otherwise qualifies for an exception to this requirement.

Examples of where the Data Transfer Restriction might apply include situations where a U.S.-based multinational needs to receive EU Personal Data relating to:

- i) **Employees or contractors of its subsidiaries in the EU** (e.g., talent management and performance data, benefits and payroll information, data related to codes of conduct or whistleblower hotlines, or other information);
- ii) **Consumers or corporate customer contacts in the EU** (e.g., customer relationship management or CRM data, or the like);

iii) **Customers’ customers or other end users in the EU** (e.g., where the multinational is an outsourcing service provider); and

iv) **Other categories of individuals** (e.g., job candidates, clinical trial subjects, business partners, or others).

As mentioned above, the European Commission has issued a decision that, if a U.S. organization self-certifies compliance to the Safe Harbor, it will be deemed to provide “adequate protection” and satisfy the Data Transfer Restriction for the duration of its participation in the Safe Harbor. In practice, an eligible organization in the U.S. can join the Safe Harbor by (i) conducting due diligence and taking the necessary steps to conform its data handling practices to the Safe Harbor rules (e.g., providing data subjects in the EU with a sufficient privacy notice, maintaining reasonable security for covered EU Personal Data, providing individuals in the EU with access to their own EU Personal Data, and taking other steps); and (ii) completing the self-certification form with the U.S. DOC. Once the organization completes the self-certification, its name and Safe Harbor registration will be published on the U.S. DOC’s list of Safe Harbor companies, and will be deemed to provide “adequate protection” for categories of EU Personal Data covered by its self-certification. After that point, any violation of the Safe Harbor rules can be subject to an enforcement action by the U.S. Federal Trade Commission.

**2. What alternative approaches could U.S. companies use to address the data transfer restriction?**

U.S. companies could also address the Data Transfer Restriction through other means, such as: obtaining express consent from the individuals at issue (Express Consent); adopting and obtaining approvals from data protection authorities for a set of binding corporate rules (BCRs); or establishing privacy agreements that conform to standard contractual clauses issued by the

European Commission (Model Contracts). A brief summary of each of these options is set out here:

i) **Express Consent.** Five or 10 years ago, many companies adopted the Express Consent approach to international data transfers, particularly with respect to EU Personal Data about employees. Today, relatively few companies are selecting Express Consent as a comprehensive solution to addressing Data Transfer Restrictions. This is due to several factors, including concerns about “drop out” rates where some individuals may not consent, and recent opinions of data protection authorities that such consents, particularly by employees, may not be “freely given” and therefore may be invalid. It is worthwhile to note that Express Consent is still a useful solution for limited or specific situations (e.g., e-commerce offerings with “accept” clicks, employee stock options, and the like).

ii) **Binding Corporate Rules (BCRs).** BCRs have received significant trade press attention lately. The concept of BCRs is attractive because a group of affiliated companies will have the flexibility to develop its own articulation of privacy rules for intra-group data flows. This allows the group to tailor the rules to its actual data flows and business culture. However, the group is not free to develop whatever rules it likes—it must still comply with guidance issued by European data protection authorities regarding the data privacy principles when developing such rules. The group must also seek substantive approvals for the BCRs from the data protection authorities in the relevant EU countries. Also, BCRs only cover intra-group data transfers, and do not cover transfers to or from unaffiliated parties (e.g., service providers, business partners, M&A parties), and in practice many companies have applied BCRs to human resources data only, due in part to the complexity of obtaining approvals for customer or other categories of data. Despite recent efforts by the European data protection authorities to streamline the approval

process, the negotiations with data protection authorities for the approval for BCRs still require time and resources and tend to discourage companies from pursuing this approach unless they have significant resources to devote to the process. There are no published statistics available as to how many companies have obtained approvals for BCRs, although latest estimates indicate that the number is less than 30.

**iii) Model Contracts.** Model Contracts have advantages in that, unlike BCRs, the terms are pre-approved by the European Commission (no substantive data protection authority approvals required). Also, unlike Express Consent, there is no need to obtain approval from affected individuals. Although Safe Harbor shares both of these advantages, Model Contracts do have certain advantages relative to Safe Harbor, including that they facilitate cross-border data transfers from the EU to jurisdictions outside the U.S. (e.g., data transfers from Europe to Asia, Latin America, and other regions and jurisdictions). Model Contracts also are not subject to enforcement by the U.S. Federal Trade Commission, and rely exclusively on local enforcement by data protection authorities and courts in the European Union. Model Contracts have certain disadvantages relative to Safe Harbor, including that a proper implementation requires the execution and maintenance of a network of intercompany privacy agreements between and among affiliates worldwide. Acquisitions or other corporate changes will trigger requirements to execute new agreements, and changes in business processes or data transfers can also require adjustments to the existing intercompany framework. In addition, the specific terms in the Model Contracts (which sometimes can be difficult to understand and follow) cannot be changed in any way without triggering a data protection consultation or approval requirement and subsequently creating a risk that the agreements will not be recognized by such authority as a valid implementation of the "model" agreement. Finally, among

the other terms, the Model Contracts contain express third-party beneficiary rights for the data subjects to sue the EU affiliate (as "data exporter") and, in certain circumstances, the U.S. parent (as "data importer") for violations of the terms of the contract. There are no precise numbers of companies that utilize Model Contracts to protect international data transfers, although the "pre-approved" nature of the agreements and their longstanding availability, combined with experience, suggests that they have been used at least as frequently as Safe Harbor to protect data transfers to the U.S.

### **3. Why would a U.S. company select the Safe Harbor?**

U.S. companies may choose to join the Safe Harbor for a variety of reasons. Several of the key driving factors may include:

#### **i) Increased demands for cross-border data transfers.**

U.S. companies are experiencing increased demands for cross-border data transfers, such as: (a) greater integration of global business operations, (b) consolidation of information technology infrastructure and support services, (c) implementation of company codes of conduct and whistleblower hotlines, (d) increased requirements to conduct global internal investigations, and to respond to government inquiries and e-discovery and litigation demands on a worldwide basis.

#### **ii) Increased scrutiny of data transfer practices.**

U.S. companies are also finding that relevant stakeholders are engaging in increased scrutiny of company privacy practices, including works councils and other employee-representative bodies, individual employees, data protection authorities, consumers, competitors, and others. This requires the companies to select and implement reliable solutions for international data transfers.

#### **iii) More flexibility for onward transfers where required by U.S. law, ordered**

*See, U.S. - EU Safe Harbor, page 6*

## **PRIVACY PREDICTIONS -2010-**

Between the FTC Roundtables, federal legislation, and HIPAA regulations, I believe privacy will be at the forefront of concerns for many companies. It will be important to follow privacy events in the EU, as well, since those may affect FTC thinking. With respect to data security, with the data breaches that occurred in 2009, unless there is clear federal preemption, I would envision more states considering specific and prescriptive data security requirements.

*—Benita Kahn, CIPP, Partner,  
Vorys, Sater, Seymour and Pease LLP*

Widespread adoption of the icon for online behavioral advertising will occur and be visible across the Internet. Progress on important legal and policy issues will occur if all interests continue to work constructively together. The public will call for more aggressive use of personal information to protect citizens against terrorism. Technology and the Information Age will reach new heights with wireless and television innovation and benefits that rely on consumer information. Public love for the Internet continues to reach new peaks.

*—Stu Ingis, Partner,  
Venable LLP*

# PRIVACY PREDICTIONS -2010-

An arousing turn of the year in the matter of privacy: At the end of 2009 Eric Schmidt, CEO of Google, told *CNBC*: "If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place." At the beginning of 2010, Mark Zuckerberg, founder of Facebook, told a live audience that if he were to create Facebook again today, user information would be public by default, not private as it was for years until the end of December.

It seems that privacy has become a disused concept. The new decade is about openness and total disclosure. Individuals and organizations will have to engage even more in protecting privacy as a rare but necessary concept for human life in the digitally networked world. Remember? Privacy has always been interpreted as a precondition for human self-determination and a free and democratic society. I don't remember any convincing argument that has made this assumption obsolete. So let's take care.

—*Miriam Meckel, Managing Director, MCM-Institute, University of St. Gallen Switzerland, and 2009-2010 Berkman Center for Internet and Society fellow*

## U.S. - EU Safe Harbor

*continued from page 5*

by a court, or necessary to perform a contract. Safe Harbor has more flexible rules than Model Contracts with respect to onward transfers to third parties. Specifically, Model Contracts prohibit the relevant company from disclosing data to third parties unless it has obtained the agreement of the recipient to abide by the Model Contract terms, or has obtained consent from individuals. Such rules may be difficult for a company to satisfy fully in the context of U.S. government demands for data, court orders in e-discovery or litigation, or data transfers that are necessary to perform a contract with the individual data subject. Similarly, the specific rules on such onward transfers in BCRs need to be negotiated on a case-by-case basis with the European data protection authorities, and may likewise be difficult to satisfy depending on the outcome of such negotiations. In contrast, the Safe Harbor provides important exceptions to onward transfer restrictions, such as for situations where the data sharing is required by a legal requirement in the U.S. (e.g., in the context of government demands for data), a court order in the U.S. (e.g., the context of e-discovery), and data sharing that is necessary to perform a contract with the data subject, or otherwise qualifies for exceptions in the Directive or national data protection laws.

### **iv) Greater control for the U.S.**

**company.** Safe Harbor provides the U.S. company (versus local affiliates) with greater control over the cross-border data transfer solution than Model Contracts and BCRs. The Safe Harbor primarily requires the U.S. company to undertake relevant compliance steps, and does not generally require significant local affiliate involvement. In contrast, Model Contracts require the participation of local affiliates in Europe to execute the intercompany agreements. On an ongoing basis, Model Contracts by their own terms provide local affiliates with audit and other rights over the U.S. companies (a situation that often does not

represent the actual hierarchical structure of a U.S.-based company and its local affiliates). BCRs require even more extensive participation of local affiliates to negotiate for substantive approvals from data protection authorities for the terms in the BCRs.

**v) Achievable and practical nature of Safe Harbor.** Safe Harbor is an achievable and practical solution because, unlike BCRs, self-certification to Safe Harbor does not require any substantive negotiations with the European data protection authorities—the U.S. DOC already completed such negotiations for the Safe Harbor rules several years ago.

### **vi) Enhanced brand reputation for outsourcing providers and satisfaction of EU customer requirements.**

Outsourcing service providers in the U.S. may find Safe Harbor participation advantageous when doing business with corporate customers in the EU (EU Customers). Among other benefits, Safe Harbor participation can help enhance the U.S. provider's brand reputation, and demonstrate to EU Customers that the provider understands EU data protection concerns. Safe Harbor participation can also help reduce the compliance burden on the EU Customers by helping them avoid the need to maintain a network of Model Contracts conforming to the European Commission "data processor" clauses. In addition, Safe Harbor participation can streamline the steps that the EU Customers need to take to comply with local data protection authority registration requirements in some countries (discussed further below in paragraph ix).

**vii) Coverage for Switzerland.** The Swiss Federal Data Protection and Information Commission (Swiss DPA) has recently established the U.S.-Swiss Safe Harbor Framework with the U.S. DOC. As a result, U.S. companies can address the cross-border data transfer restriction in the Swiss data protection law by self-certifying compliance to the Safe Harbor rules, in the same way as can be done for transfers from the EU. This development is particularly impor-

*“The FTC has recently taken its initial enforcement actions pursuant to the Safe Harbor.”*

tant for Switzerland, as the definition of “personal data” under Swiss law covers identifiable information regarding individuals and legal entities, making personal data protections provided under Swiss law broader than those of many EU member states, which generally only protect identifiable information regarding natural persons.

viii) **Better fit for “online” data collections.** The Safe Harbor is better suited to protect online transfers of data because the U.S. company would not need to obtain an express consent from Web site visitors for the data transfers, and would not need to enter into contracts with entities in the European Union (both of which may be cumbersome depending on the business model or application). Instead, the Safe Harbor would require the U.S. company to confirm that its privacy policy and privacy practices adhere to the Safe Harbor rules—a step that may be easier for companies to administer in the online context than obtaining Express Consent or executing Model Contracts.

ix) **Streamlining of local filing procedures.** In a number of EU member states, cross-border transfers of EU Personal Data may trigger registration requirements with the data protection authorities. In some of these countries, the Safe Harbor facilitates the local registration process by avoiding “procedural” approvals that apply to use of Model Contracts and the “substantive” approvals for BCRs. For example, in Spain, the use of Model Contracts attracts certain requirements for special notary and other procedural approvals when the local company registers with the data protection authority. This

requirement is not triggered when the data recipient is a U.S. company that self-certifies with the Safe Harbor.

x) **Avoiding administrative burdens of maintaining Model Contracts.** Model Contracts must be monitored to make sure that they reflect changes in the relevant company’s structure. By contrast, particularly in the context of mergers and acquisitions, as well as other business changes and developments, Safe Harbor avoids the administrative burden of negotiating and executing new Model Contracts to cover new affiliates and data flows.

#### **4. Why would a U.S. company choose a data transfer solution other than the Safe Harbor?**

Although there are many good reasons to join Safe Harbor, or use Safe Harbor as a baseline to authorize certain data transfers, there are good reasons why Safe Harbor may not be sufficient for all data transfers, and why a company might choose alternative approaches.

i) **FTC enforcement.** The promise to comply with Safe Harbor is ultimately subject to the enforcement authority of the FTC. The FTC has recently taken its initial enforcement actions pursuant to the Safe Harbor. In the first case, the FTC obtained a Temporary Restraining Order (TRO) in the United States District Court for the Central District of California enjoining a consumer electronics company (Consumer Electronics Company) from engaging in a broad range of unfair and deceptive practices related to online consumer sales, including misrepresenting that the company participated in Safe Harbor. According to the FTC complaint, the Consumer Electronics Company had, at various times, advertised on its Web sites that it had self-certified to the Safe Harbor, even though it had never done so. The FTC complaint also alleges that the company had engaged in a wide variety of other unfair and deceptive practices relating to commercial practices, such as: (i) failing to notify consumers

*See, U.S. - EU Safe Harbor, page 8*

start page  
Protests in Iran

WISH YOU HAD  
**SEARCH ENGINE  
PRIVACY?**

Major search engines log every web search you do. They may hold sensitive data about you and your client's health, political views, job searches, legal issues, intellectual property and more.

As a privacy professional, shouldn't you be concerned?

It's time to switch to

**start  
page**.com  
By Ixquick

**100% PRIVACY  
GREAT SEARCH RESULTS  
NO IP ADDRESSES LOGGED  
THIRD-PARTY CERTIFIED**

**Start protecting your company  
Start protecting your clients  
Start protecting your co-workers  
Start protecting yourself**

**THE WORLD'S MOST  
PRIVATE SEARCH ENGINE**

# PRIVACY PREDICTIONS -2010-

## Privacy in the healthcare sector, 2010

The concept of de-identified data as a privacy protection will be challenged by multiple stakeholders; the results of this discussion will be critical to healthcare privacy and related federal laws (e.g., HIPAA, HITECH). There will be those who are concerned about the risk of re-identification, there will be those espousing de-identification as being more protective of patients than handling protected health information (PHI) directly and while accomplishing the same goals, and there will be regulators involved in trying to find common ground that satisfies conflicting interests. Ultimately, I suspect that de-identified data will prevail as a better alternative to using PHI in the healthcare sector, albeit with a more regulated security network around it.

—Kim Gray, Chief Privacy Officer,  
Americas Region, IMS Health

In the field of advertising in 2010, the mobile Internet will finally become the new frontier for user data collection and analysis, and the use of Flash cookies on the Web will likely re-ignite the debate on third-party tracking devices.

—Fernando Bermejo  
Associate Professor of  
Communication at Universidad Rey  
Juan Carlos in Madrid, Spain and  
2009-2010 Berkman Center for  
Internet and Society fellow

## U.S. - EU Safe Harbor

*continued from page 7*

about applicable customs duties and other taxes; (ii) frequently shipping products that did not comport to customer orders and that had power chargers that were incompatible with local power systems where the consumer was located; (iii) delivering user manuals and electronics controls that were in Spanish or Chinese entirely; (iv) charging consumer credit cards without providing the products ordered; and (v) failing to disclose warranties and other material terms. In addition to the TRO, the FTC seeks further relief in the form of a permanent injunction, restitution, disgorgement of profits, and other equitable relief.

In a second set of enforcement actions, the FTC agreed to settle cases with six U.S. businesses that allegedly falsely claimed that they participated in Safe Harbor. The FTC complaints charged World Innovators, Inc.; ExpatEdge Partners LLC; Onyx Graphics, Inc.; Directors Desk LLC; Collectify LLC; and Progressive Gaitways LLC (the "Safe Harbor Six") with representing that they held current certifications to the Safe Harbor program, even though the companies had allowed their certifications to lapse. Under the proposed settlement agreements, the Safe Harbor Six are prohibited from misrepresenting the extent to which they participate in any privacy, security, or other compliance program sponsored by a government or any third party. The FTC did not assess any fines in connection with these settlements.

These cases are important because they represent the first enforcement actions the FTC has taken under Safe Harbor since the inception of the program in November 2000. It may signal that the FTC will be more active in pursuing Safe Harbor cases in the coming months, and that companies should be even more diligent in confirming that they comply with the Safe Harbor rules before completing a self-certification.

**ii) Data transfers not eligible for coverage by Safe Harbor.** U.S. companies are only eligible to join the Safe Harbor

to protect certain transfers of EU Personal Data to the United States. Other transfers within a global enterprise, such as transfers from the EU to Asia or Latin America, are not covered by Safe Harbor. Likewise, financial institutions and other organizations that fall outside the scope of FTC and DOT authority are not eligible to join Safe Harbor, even if the organizations are located in the United States. This "coverage" issue is perhaps one of the most significant reasons why companies may utilize other approaches.

**iii) Development of tailored privacy compliance programs.** U.S. companies that already have well-established global data protection programs may wish to consider developing more tailored company-wide data protection compliance programs through BCRs. Such companies can build on the controls that they have already established under Safe Harbor and/or Model Contracts, and develop rules and procedures that address the guidance issued by the data protection authorities on BCRs, while tailoring such terms to the group's actual data flows and handling practices. In the interim period while the group of companies seeks approval for BCRs, they can continue to rely on their existing data protection framework.

## 5. What are the current trends in international data transfers?

Although there are still a wide variety of practices, certain trends are emerging with respect to international data transfers. First, common industry practice has moved away from reliance on a broad "waiver" of privacy rights through Express Consents, particularly in the employment context. Second, although BCRs are up and coming, the burdens of negotiating for substantive approval from data protection authorities and other factors may place this solution out of reach for many U.S. organizations, except for companies that already have well-developed global privacy programs based on Safe Harbor or Model Contracts.

Third, the "work horses" for compliant international data transfers in the cur-



rent environment appear to be Safe Harbor and Model Contracts. Companies entering the “global privacy compliance” market for the first time at the enterprise level often select between these two solutions. Key considerations in favor of Safe Harbor include more flexibility with respect to onward transfers (e.g., to government authorities in SEC or other government investigations, as well as to other parties in e-discovery and litigation), greater control for the U.S. parent company, the avoidance of the maintenance of a network of intercompany privacy agreements, and the avoidance of express third-party beneficiary rights for data subjects. Key considerations in favor of Model Contracts are the avoidance of FTC enforcement authority, and the ability to cover data transfers from the EU to non-U.S. jurisdictions (e.g. Asia or Latin America).

Ultimately, there is no one-size-fits-all solution. Companies make strategic decisions on cross-border privacy solutions based on their own particular situation, including worldwide data flows,

*“...Companies are finding they benefit from a period review to confirm that the global ‘privacy house’ is in order...”*

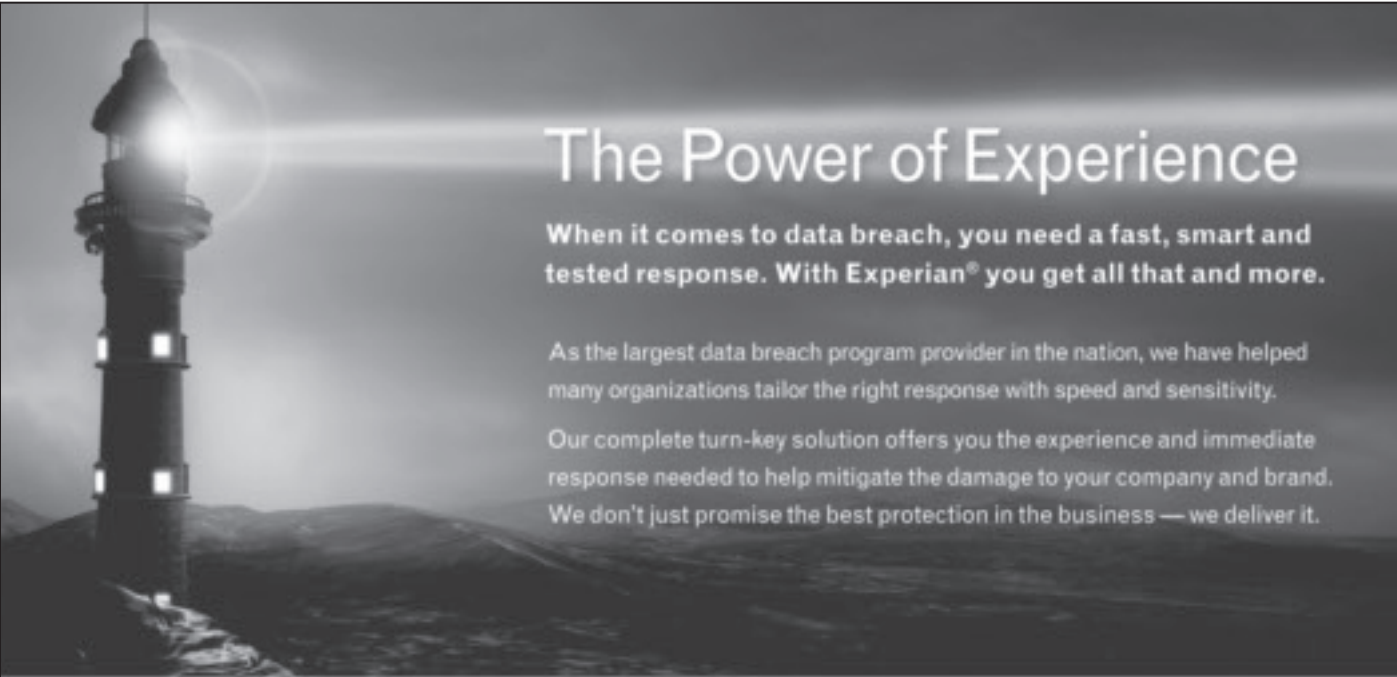
compliance issues, business operations, litigation experience, and other factors. One trend that is unmistakable, however, is that companies today operate in an increasingly interconnected world and, for enterprise risk management purposes, are finding that, at a minimum, they benefit from a periodic review to confirm that the global “privacy house” is in order and responsive to the latest risks and privacy regulatory developments.

*Brian Hengesbaugh, CIPP, is a partner in the Chicago office of Baker & McKenzie. He concentrates on domes-*

*tic and global data protection, privacy, and information security, and is a member of the firm’s Global Privacy Steering Committee. Mr. Hengesbaugh is a past member of the IAPP Publications Advisory Board. Prior to joining Baker & McKenzie, Mr. Hengesbaugh served as the lead attorney for the U.S. Department of Commerce General Counsel’s Office in the negotiation of the U.S. - EU Safe Harbor Privacy Framework.*

*Michael Mensik is a partner in the Chicago office of Baker & McKenzie, concentrating on information technology, sourcing, and privacy. He was recently elected to the Outsourcing Hall of Fame by the International Association of Outsourcing Professionals.*

*Amy de La Lama is a senior associate in the Chicago office of Baker & McKenzie, concentrating on domestic and global data protection, privacy, and information security.*



## The Power of Experience

When it comes to data breach, you need a fast, smart and tested response. With Experian® you get all that and more.


As the largest data breach program provider in the nation, we have helped many organizations tailor the right response with speed and sensitivity.

Our complete turn-key solution offers you the experience and immediate response needed to help mitigate the damage to your company and brand.

We don't just promise the best protection in the business — we deliver it.

**VISIT** [experian.com/databreach](http://experian.com/databreach) for more information.

**CALL** Experian's data breach experts at (866) 751-1323 for your free consultation.



# 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*

**Learn**  
at more than 70 sessions  
**Network**  
with the global privacy community  
**Join**  
the world's largest gathering of privacy professionals



**THE IAPP GLOBAL  
PRIVACY SUMMIT 2010**

**April 19 - 21  
Washington, DC**

**Register Now**  
[www.privacysummit.org](http://www.privacysummit.org)

## The IAPP Welcomes our Newest Corporate Members



**Jordan Lawrence™**



An MLF Financial Group Company

**MapleLife**  
FINANCIAL INC.

Looking at LIFE in a new light™

A Maple Life Financial/Cantor Fitzgerald Company

**MLF LEXSERV™**

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

## PRIVACY PREDICTIONS -2010-

Privacy protection will remain a very important subject of the lobbying efforts by the marketing industry in 2010. The media will continue to be extremely alert to suspected violations of data protection and it is a fact that even after enactment of the Data Protection Law reform in Germany on September 1, 2009, consumer data will still be misused—contrary to what the government and the consumer protection agencies promised. This corroborates our statement which we have ever since repeated, like a mantra: the so-called “privacy scandals” are not a matter of loopholes in the law but of poor enforcement of the existing laws.

Since the new German government is in place, employee privacy and online privacy have become important matters, also. In November 2009, a draft for an Employee Privacy Act was submitted to the German Bundestag.

Moreover, a considerable level of uncertainty remains that marketers’ use of personal data could be placed on the agenda of lawmakers again in 2010.

How will these developments affect the core activities of our members—the reputable businesses with “address data”? The German Federation of Direct Marketing will continue campaigning for a cautious and balanced approach to further data protection law reforms.

—Dieter Weng, President of the German Federation of Direct Marketing (DDV e.V.)

## Managing global data privacy

By Paul M. Schwartz

Successive revolutions in information technology raise new challenges, risks, and opportunities for consumer privacy protection. Perhaps the most basic question is how these new technologies are changing the actual practices of companies in processing personal information. After all, emerging technologies can make legal regulations obsolete or out-of-date. The consequences can be ineffective regulation and a waste of corporate resources without meaningful protections for consumer privacy.

To understand the impact of new technologies on company practices and legal regulations, I researched how six leading North American companies manage their global use of personal information. This work was sponsored by the Privacy Projects, a new nonprofit organization devoted to empirical research into privacy issues.

My whitepaper, *Managing Global Data Privacy*, looks at companies that are developing pharmaceuticals, providing marketing, selling financial services, and offering a range of Internet-based software, technology, and online services. These companies collect and process personal information about clinical health research, customer services, consumer surveys, mortgage renewals, e-mail accounts, and global job applicants.

The resulting case studies identify three dramatic changes from the world of yesterday. The first change shown is that the scale of global data flows in the private sector has increased massively. In the recent past, an international exchange of personal information was a rare event that the law tended to regulate on a case-by-case basis. But personal information now flows around the world 24/7. The volume is staggering—one company in the study created more than five million data points in 2008. This figure represents 72 new data points every minute.

Second, the nature of this constant flow of global data is dynamic and occurs across borders. In the past, companies

finalized international data transfers in advance. Personal data were sent at a single moment from one central location to another. Today, companies draw on “the cloud” to put computer resources and services on the Internet. As a result, the processing of personal data increasingly takes place simultaneously throughout a global network.

Third, the oversight of data flows at these leading companies has been professionalized with a significant investment of business resources. This development is highly promising. In the past, many corporations avoided privacy and security issues and devoted a low level of resources to them. Companies now are creating collaborative processes for privacy and security, which involve chief security officers, chief privacy officers, legal counsel, and internal management boards.

One regulatory lesson to be drawn from these studies is to question the value of the approach in certain European countries that require registrations for any data processing operation involving the personal information of citizens. Even a minor change in the location of a single server, or an alteration of a single process will require costly modifications to existing registrations in different European countries. Yet, in the age of dynamic and massive data flows carried out on “the cloud,” such changes can frequently occur. Moreover, it is far from clear that the benefit for individual privacy, if any, is equal to the cost of making companies file detailed, national-specific reports on each database that contains personal information.

---

*Paul M. Schwartz, CIPP/C, is professor of law, Berkeley Law School, U.C.-Berkeley, and a director of the Berkeley Center for Law & Technology. His whitepaper, Managing Global Data Privacy, is available at: <http://theprivacyprojects.org/privacy-projects>.*

## Privacy and pandemic planning: a few prudent considerations for organizations

By Rachel Hayward, CIPP/C

As the international community readies itself for a second wave of the H1N1 flu pandemic, wise organizations are brushing off their business continuity plans (BCPs) and reviewing their applicability to a different kind of threat. Unlike traditional business continuity or disaster recovery planning, pandemic planning requires management for a prolonged but unidentified period of time rather than for the single risk event that traditional business continuity planning tends to focus on. The focus of pandemic planning is on the people within an organization rather than buildings, structures, or environmental. Shifting the focus of your BCP to incorporate the organization's employees requires a gentle reminder that the privacy of employees must remain paramount, even during business continuity management.

Privacy professionals must remain vigilant in the wake of the H1N1 flu pandemic to ensure the privacy rights of employees remain intact during pandemic response activities. An all-hazards approach to business continuity planning in combination with taking a few common-sense approaches to privacy, will assist in easing the stress of the flu pandemic on organizations.

Privacy professionals need to work with the business continuity planners and human resource departments to clarify any questions regarding the collection, use, and disclosure of personal employee information during the development of organizational BCP plans that include considerations for pandemic planning. The challenge is to balance these needs with the needs of the organization to plan for the potential of prolonged staff shortages caused by employee illness, and, potentially, employees staying home from work to care for loved ones. Due to the way in which the illness spreads, a single department within an organization may

be severely affected while other areas are less affected, or not affected at all.

During times of crisis, management organizations may be tempted to collect a variety of information from staff, such as their diagnoses and whether they have received the H1N1 vaccine. Jurisdictional privacy legislation may, however, prevent this collection. In Canada, for example, this is likely not a reasonable collection of information under provincial or federal privacy legislation.

Organizations may be tempted to use personal information contained in HR files, such as the number of dependents within staff members' households or personal contact information for pandemic planning or response purposes. This may pose a privacy threat to staff and a legislative or policy breach to organizations. Finally, organizations may be tempted to disclose information about staff that they would not normally consider disclosing in non-pandemic situations, such as an employee diagnosis or reason for an employee's absence at work. Privacy professionals can, instead, urge their organizations to consider a twofold approach that focuses on information dissemination and careful pre-planning to manage the flu pandemic.



Rachel Hayward

An informed employee has the information he needs to care for himself and his family members. Organizations can provide their staff with information regarding safe hand washing and other basic flu prevention techniques, as well as local government hotlines or other resources to help them

understand the best flu prevention methods. If the flu vaccine is available in your area, consider posters in common areas with contact information on how and where they can receive the vaccine. A thorough communication plan will empower employees to manage their own risks, as well as those in their family, and in turn keep everyone healthy and at work.

Empowering employees with critical information regarding the H1N1 flu virus can be combined with the implementation of some basic policies and techniques to be used within the office. Offering hand sanitizer in break and meeting rooms and asking employees to stay home when they are sick are two simple methods that can be used to further reduce the infection rates in the workplace. Clear communication with employees is a key element in pandemic preparedness.

Perhaps the most important privacy protection during a pandemic is a properly tailored all-hazard business continuity plan that requires little or no additional collection, use, or disclosure of employee information. A holistic approach that identifies potential risks and their impacts to business operations, including the risk of a pandemic, will provide an organization with the tools it needs to respond to such a crisis. Specifically, the plan should consider prolonged staff

*“Perhaps the most important privacy protection during a pandemic is a properly tailored all-hazard business continuity plan that requires little or no additional collection, use, or disclosure of employee information.”*

See, *Pandemic planning*, page 16

## Turning 10 in 2010

The IAPP celebrates its tenth anniversary this year. To commemorate, the *Privacy Advisor* will look back at some of the decade's most memorable moments, achievements, and milestones. We start with a look inward.

The *Privacy Advisor* is valuable because of you, the experts in the field who so willingly share your knowledge with IAPP members. Of course, some of you are more prolific than others.

We dusted off the archives to determine just who has been most

profuse. One byline came up time and time again. Philip L. Gordon, Esq., contributed his first story back in 2003 when the newsletter bore a different name. It was about options for employers facing the HIPAA Transaction Rule compliance deadline. Hopefully you're all compliant by now. If not, call Phil. He is a shareholder and chair of the Privacy Task Force at Littler Mendelson, P.C. in the Mile High City.

Thank you, Phil, for sharing so much valuable information for the good of the privacy profession.

## Pandemic planning

*continued from page 15*

shortages rather than the traditional disaster planning approaches that tend to focus only on the infrastructure of an organization and its ability to detail a specific timeline for the full resumption of business. Critical process and position identification, properly aligned with well-rounded policies and procedures and an appropriate plan for full or partial plan implementation will best serve an organization during a flu pandemic. Careful pre-planning that is flexible and adaptive will reward employers when faced with a flu pandemic or other unexpected disruption to their business.

Prior to deciding to collect, use, or disclose personal employee information in an attempt to manage a pandemic situation, organizations need to understand the requirements of the privacy legislation by which they are bound. It is advisable to seek the assistance of privacy professionals. Organizations need to carefully plan their response to a pandemic and consider the careful balance between the protection of employee privacy and the continuation of business. Privacy professionals must remain vigilant in their quest to protect personal information and must be prepared to advise their organizations when plans may infringe on the privacy rights of employees.

The federal privacy commissioner of Canada and the information and privacy commissioners of the provinces of Alberta and British Columbia recently released a publication titled "Privacy in the Time of a Pandemic," to assist organizations in working through some of these issues. The article can be found at [www.oipc.ab.ca/Downloads/document-loader.ashx?id=2492](http://www.oipc.ab.ca/Downloads/document-loader.ashx?id=2492)

*Rachel Hayward is a privacy and information management specialist and the information risk management lead for the Edmonton, Alberta Deloitte Office. She holds a masters degree in public administration and became a CIPP/C in 2007.*

# Learn the latest on privacy without ever leaving your office.

Visit the IAPP's online Educational Library.

FEATURED AUDIO CONFERENCE



### *Global Privacy and the Endless Entanglements of U.S. Laws*

Dealing with the legal complexities of managing data across international borders? Find out what you need to know about litigation strategy, internal and external investigations, and data strategies to stay on top of your most challenging global privacy management concerns.



Buy it today at [www.privacyassociation.org/edulibrary](http://www.privacyassociation.org/edulibrary)



# The Lisbon Treaty and data protection: What's next for Europe's privacy rules?

By Daniel Cooper, Henriette Tielemans, and David Fink of Covington & Burling LLP's Privacy and Data Protection Practice Group

*This article originated as a Covington & Burling LLP Privacy & Data Protection Advisory and is reprinted here with permission.*

**T**he Lisbon Treaty entered into force on December 1, 2009. This agreement substantially overhauls the EU's legal bases, the Treaty on European Union (TEU), and the Treaty Establishing the European Community (EC Treaty), the latter of which is renamed the Treaty on the Functioning of the European Union (TFEU). While much attention has been given to the Lisbon Treaty's reform of the EU's institutional arrangements, it also alters the legal grounds for legislation in the data protection area in ways that could impact privacy regulation. Below, we describe the key changes and consider the potential effect on Europe's data protection framework.

## Data protection under the current treaties

To date, EU data protection laws have been primarily based on provisions in the EC Treaty empowering the EU to legislate in furtherance of the internal market. Both the landmark Data Protection Directive (95/46/EC) and the e-Privacy Directive (2002/58/EC) were promulgated on this basis, and, consequently, they concern both protection of privacy and the free movement of personal data. Two other provisions also play a role. Article 30(1)(b) TEU requires that transfers of law enforcement information be subject to appropriate data protection measures, and this was the principal basis for Framework Decision 2008/977/JHA. In addition, Article 286 EC Treaty provides for the application of data protection rules to the EU Institutions and for the establishment of



Daniel Cooper



Henriette Tielemans



David Fink

an independent body to oversee data protection in this context (this led to the creation of the European Data Protection Supervisor).

## The new provision on data protection: individual rights and expanded EU authority

The most striking change for data protection under the Lisbon Treaty is a new, prominent provision on the subject—Article 16 TFEU—which replaces and expands on the old Article 286. Article 16 states as follows:

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

What does this mean for data privacy? First, the provision establishes an explicit right to data protection. It appears that this right would be directly applicable to persons, and that they could consequently invoke it in court. The right to data protection is reinforced by the revised Article 6 TEU, which provides

that the EU Charter of Fundamental Rights "shall have the same legal value" as the TEU and the TFEU. This would seem to have the effect of incorporating directly into EU law all of the rights in the Charter, including Article 8 on the Protection of Personal Data. Article 8 contains language essentially identical to clause 1 of Article 16 TFEU, and additionally establishes rights to fair processing of personal data, access to such data, and rectification. The Data Protection Directive already provides that Member States should ensure similar protections.

Second, clause 2 of Article 16 establishes a clear basis for the Council and Parliament to regulate the processing of personal data by Member State authorities when carrying out activities that fall within EU law, in addition to the EU Institutions previously covered by Article 286. But the full scope of this clause is not entirely clear. One could interpret the phrase "and the rules relating to the free movement of such data" as granting the Council and Parliament a general right to legislate data protection rules, including for the private sector. This is not, however, the most obvious reading of the text, which instead seems to refer to regulation of the free movement of personal data among public authorities in Europe. Furthermore, there does not appear to be any reason why the EU could not continue to regu-

*See, Lisbon Treaty, page 18*

*Lisbon Treaty*

*continued from page 17*

late data protection in the private sector on the basis of internal market provisions.

Finally, the last sentence of clause 2 references a carve-out for data protection rules in the context of the common foreign and security policy. Under Article 39 TEU, the council, alone, is empowered to adopt rules on the processing of personal data by Member States in this area.

**The abolition of the pillar structure and its impact on data protection in law enforcement activities**

One of the key structural reforms of the Lisbon Treaty—the abolition of the pillar system—could also affect privacy rules. Pre-Lisbon, the EU comprised three legal pillars with separate legal bases for legislative action: (i) “Community” matters; (ii) Common Foreign and Security Policy; and (iii) Police and Judicial Cooperation in Criminal Matters. Crucially, only the council was empowered to adopt legislation in the third pillar on data protection, pursuant to Article 30(1)(b) TEU.

With the elimination of the pillar structure, it appears that any future laws on data protection in the police and judicial context would be based on Article 16 TFEU, where both the council and the Parliament are co-legislators. But some privacy advocates argue that Framework Decision 2008/977/JHA must also be revised—with input from the Parliament—to reflect the co-legislation requirement, or, alternatively, that the Data Protection Directive must be amended to encompass the use of personal data by police and judicial authorities (this would also involve co-legislation by the council and Parliament). Others, however, might argue that a change in the procedure for adopting legislation does not require the re-opening of laws validly adopted under an old procedure. It remains to be seen how this will play out.

**New international privacy principles for law enforcement and security**

*By Mary Ellen Callahan, CIPP*

Cross-border data flows have long been a subject of global dialogue. In the late 1970s, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe began to explore cross-border transactions, with OECD issuing the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, and the Council of Europe issuing the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. In 1990, the United Nations adopted the Guidelines for the Regulation of Computerized Personal Files. In 2004, the Asia Pacific Economic Cooperation issued its Privacy Framework. All four guidelines apply to the public sector, although they also include exemptions for law enforcement and security, which remain prevalent in national and European law.



*Mary Ellen Callahan*

Exemptions for law enforcement and security did not occur because of a dearth in sharing in this area, nor for the desire to limit law enforcement cooperation, but were necessary to protect legitimate individual cases. Almost every country with the capability of doing so exchanges information on at least a case-by-case, if not routine basis. None of these guidelines explicitly address exchanges between police working together on an investigation, which are guided by individual officers’ applications of domestic law. As a result, sharing between countries traditionally occurred on the basis of trust and mutual recognition, built on long-standing relationships between allies, or has been governed by broad cooperation agreements that give scant detail to privacy protections.

With the extensive increase in both international travel and security risks,

there has been proportional growth in the need to share larger amounts of personal data for law enforcement and national security purposes. Data protection laws have also grown in complexity and sophistication. As a result, countries need to follow the lead of the private sector and provide greater transparency

on privacy protections for data flows in the law enforcement and security context. Last month saw a landmark achievement in this area: U.S. and EU recognition of a set of core privacy principles for law enforcement and security.

**The U.S.-EU High Level Contact Group**

On October 28, officials representing the U.S. Departments of Homeland Security, Justice and State, together with the EU Presidency (represented by the Swedish Justice Minister) and the Vice President of the EU Commission, culminated almost three years of work by acknowledging the completion of the so-called High Level Contact Group (HLCG) principles. While the HLCG principles are not by themselves a binding agreement, this public acknowledgement reflects U.S.-EU shared values of democracy, rule of law, and respect for human rights and fundamental freedoms and the consequent commitment to effective data protection. These core principles will not only be the basis of future information-sharing agreements between the EU and the U.S., but will hopefully raise the standard for information sharing in the law enforcement and security context for the rest of the world.

There has long been an exchange of information between the EU member states and the U.S. for law enforcement and security purposes, resulting in numerous prosecutions. Most information sharing has occurred without contro-

versy and without a single complaint of violation of the previously mentioned standards. However, the EU's growing authority in border and security matters vis-à-vis the member states changed the context of cooperation. The information-sharing relationship with the U.S. appears to have become part of the evolving political dynamic between the EU and its member states. For example, the EU's Data Protection Framework Decision, adopted to protect privacy when European authorities share data among themselves, is prejudiced against the cooperation with non-EU partners. Likewise, the laws governing EU data systems for asylum seekers and border control (Eurodac and the Schengen Information System, respectively) restrict the transfer of data to third countries for legitimate law enforcement purposes. Unfortunately, in the name of protecting privacy, these restrictions negatively impact the equally legitimate activities of law enforcement to investigate and fight crime and terrorism.

The HLCG was formed in late 2006 to start discussions about privacy in the exchange of information for law enforcement purposes as part of a wider reflection between the EU and the U.S. on how best to prevent and fight terrorism and serious transnational crime. Composed of senior officials from the European Commission, the European Council Presidency, and the U.S. Departments of Homeland Security, Justice, and State, the goal of the HLCG was to explore ways to enable the EU and the U.S. to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. In October 2009, the group concluded the first step of that goal, producing a text that identifies the fundamentals or "common principles" of an effective regime for privacy. The next step will be for both sides to seek a binding international agreement.

The HLCG principles on privacy and personal data protection for law enforcement purposes apply in the EU for the prevention, detection, investigation, or

*"As these principles are applied, the role of privacy authorities on both sides of the Atlantic will be to ensure that the relevant organizations are held accountable to them."*

prosecution of any criminal offense, and in the U.S. for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations.

#### The HLCG data privacy principles include:

1. Purpose specification/purpose limitation
2. Integrity/data quality
3. Relevant and necessary/proportionality
4. Information security
5. Special categories of personal information
6. Accountability
7. Independent and effective oversight
8. Individual access and rectification
9. Transparency and notice
10. Redress
11. Automated individual decisions
12. Restrictions on onward transfers to third countries

Other HLCG principles addressed issues pertinent to the transatlantic relationship, including:

1. Private entities' obligations
2. Preventing undue impact on relations with third countries
3. Specific agreements relating to information exchanges
4. Issues related to the institutional framework of the EU and the U.S.
5. Equivalent and reciprocal application of data privacy law

The full text of the HLCG principles is available at [http://useu.usmission.gov/Dossiers/Data\\_Privacy/Oct2809\\_SLCG\\_principles.asp](http://useu.usmission.gov/Dossiers/Data_Privacy/Oct2809_SLCG_principles.asp).

#### Implementation

Of course, identification of common principles and incorporation into a binding agreement does not end the obligations of the parties in providing privacy protection. As these principles are applied, the role of privacy authorities on both sides of the Atlantic will be to ensure that the relevant organizations are held accountable to them. Beyond a binding agreement, we may expect joint projects to include identification of best practices for ensuring accountability, such as assessments of decision-making frameworks for the collection and use of personal information, "privacy by design" tools, and privacy enhancing technologies (PETs). A practical, outcomes-driven focus would be a welcome contribution to law enforcement and security agencies throughout the world who adopt the HLCG principles.

---

*Mary Ellen Callahan is the chief privacy officer of the U.S. Department of Homeland Security. Together with her colleagues from the Departments of Justice and State, she participated in the discussions related to the final HLCG principles. She wants to thank her International Privacy Policy Directors, **Shannon Ballard** and **Lauren Saadat**, for their assistance in the HLCG generally, and with this article, in particular.*

# U. S. FTC holds first of three privacy roundtable events and signals policy shift

By D. Reed Freeman, Jr., CIPP, and Julie O'Neill of Morrison & Foerster

*This article originated as a December 15 Morrison & Foerster Client Alert and is reprinted here with permission.*

## First FTC roundtable on privacy: December 7, 2009, in Washington, DC

### Background

The Federal Trade Commission (FTC) held the first in a three-part series of one-day roundtable meetings focused on privacy on December 7, 2009, in Washington, DC. These events are designed to bring together a variety of participants from industry, consumer advocacy organizations, trade associations, think tanks, academia and elsewhere, each with a strong interest in helping to shape the commission's approach to privacy regulation and enforcement.

The panel discussions during this first event featured vigorous debate and little consensus among industry, academic, and advocacy representatives. In sum, as explained in greater detail below, industry members urged continued self-regulation based on principles of notice and choice. They tended to consolidate around the Self-Regulatory Principles for Online Behavioral Advertising backed by the Direct Marketing Association (DMA), Interactive Advertising Bureau, Association of National Advertisers, the American Association of Advertising Agencies, and the Council of Better Business Bureaus (The DMA Program), which include enhanced notice coupled with increased consumer education, as well as principles addressing consumer control, data security, material changes, sensitive data, and accountability.

Consumer advocates, on the other hand, largely argued that both self regulation and the notice-and-choice approach had failed, and most called for new laws or rules, either alone, as a baseline for those who do not adhere to



D. Reed Freeman, Jr.



Julie O'Neill

strong self-regulation, or in addition to the DMA Program.

Commission Chairman Jon Leibowitz opened the meeting by declaring that this is "a watershed moment in privacy" because companies continue to develop more and more sophisticated technologies to collect information from consumers and use it in new ways, without consumers necessarily understanding any of this. Accordingly, he said, it is an appropriate time for the commission to take a broad look at the subject. He went on to remark that the commission's two prior approaches to privacy—the notice and choice regime and a harm-based approach—had not been as successful as the currently-constituted commission would like, and, accordingly, that the commission is searching for a new paradigm for privacy regulation and enforcement. The director of the Bureau of Consumer Protection (BCP), David Vladeck, echoed Chairman Leibowitz, but, at the same time, seemed to be more openly receptive to legislation or regulation.

### Take-Away

Although it's not yet clear how the commission will proceed, it was possible to glean some hints of where the commission could be heading. Based on this first roundtable event, it appears unlikely that the FTC will make any radical policy decisions at this point. The likely immediate result of the three events will be a staff

report outlining a new framework, although it is possible that, as in 2000, the commission or its staff will prepare a report to Congress with certain recommendations, including, potentially, a call for new legislation. Were it to make a radical change in policy now, such as requiring opt-in for behavioral advertising or applying principles of the Fair Credit Reporting Act (FCRA) to databases not now subject to FCRA (as the World Privacy Forum and other advocates have called for), the commission may find itself not just ahead of the business community, but also Congress.

As the commission learned nearly two decades ago, getting ahead of Congress is dangerous business. The last time the commission did so, in connection with a proposed trade regulation rule that would have curtailed television advertising to children, Congress reversed the FTC and ultimately reduced the commission's authority and funding. For this reason, we think the commission will continue to build a record on privacy, especially where there appear to be gaps between consumer expectations and business practices, so that it is well-poised at the conclusion of the three-part series to adopt a new interpretation of the requirements of the FTC Act and an accompanying enforcement position or to recommend new legislation it thinks appropriate based on the record.

In the meantime, we expect that the commission is likely to keep an eye on the roll-out of the DMA Program, including the extent to which it is adopted by industry, and to pursue enforcement actions against those that do not join, those that join and do not comply, and those that engage in fringe activity, such as collecting sensitive information like health, financial, or children's data for use in behavioral advertising.

*See, FTC roundtable, page 22*



# Our focus is Privacy... but our blog is open for discussion



**Proskauer's Privacy and Data Security Practice** is an outgrowth of our Internet, intellectual property, labor and employment, health care, First Amendment, international law and litigation practices. Indicative of our *Chambers USA* ranked experience and reputation in this relatively new field of law, is the fact that the venerable *Practising Law Institute* (PLI) asked our firm to create its first-ever treatise on the subject of privacy and data security law, called "Proskauer on Privacy," published in 2006. For more information about this practice area, please visit [www.proskauer.com](http://www.proskauer.com).

Subscribe to our Privacy Law Blog at

<http://privacylaw.proskauer.com/index.xml>

Proskauer

**FTC roundtable***continued from page 20*

We also expect the FTC to continue its program using its authority under Section 5 of the FTC Act to enforce against those who fail to disclose material information about (1) the collection, uses, and disclosure of data outside the privacy policy in a clear and conspicuous way, especially in the case of sensitive information, and (2) disclosures and uses of data for purposes other than that for which the consumer provides the information in the first instance.

**Roundtable debate**

We have structured our summary of the roundtable discussions around the two primary themes of the debate about where the commission's approach to privacy should head: (1) whether the notice-and-choice regime remains viable; and (2) how to evaluate and respond to the harms associated with information practices.

**Is the notice-and-choice regime dead?**

Chairman Leibowitz stated that, in the commission's view, the notice-and-choice approach to privacy has not succeeded. He explained that he has long been a proponent of opt-in (versus opt-out) choice to the collection of personal information, but he pointed out that even that can fail if notice is inadequate. He further explained the inadequacy of notice and choice with his statement that "we all agree" that consumers don't read privacy policies or EULAs.

**Advocates' positions**

Many consumer advocates agreed with the chairman, taking the position that choice is illusory when consumers—even when given notice—have no way to fully understand the complicated technology used to collect information from them, the extent of the data collected, and the variety of uses and disclosures made of it, including, sometimes, undisclosed secondary uses. In their view, no notice can be sufficient in this context. They also argued that regulators and industry have focused on notice and choice when they

should instead focus on the substance of information practices, i.e., ensuring that personal data is collected and processed fairly. For these reasons, consumer advocates largely encouraged reliance on a full set of Fair Information Practices principles (FIPs) (not just notice and choice) to craft legislation, regulation, or, at least, a regulatory policy framework. In their view, the FIPs require, among other things, opt-in consent to information collection and the consumer's ongoing ability to control how his or her information is used and shared.

Some advocates, such as the World Privacy Forum, also called for the protections of the Fair Credit Reporting Act to be applied to marketing databases that are not now subject to FCRA. BCP Director Vladeck noted that the data broker industry is largely unknown and may warrant attention; if the commission follows the recommendation of the World Privacy Forum, it would mark a dramatic departure from current industry practices.

**Industry response**

Not surprisingly, industry representatives took an opposing view. They believe that industry has provided, and continues to work on ways to improve appropriate notice, as well as tools that consumers can use to exercise control over their data. They acknowledged the need to continue with consumer education efforts and noted the steps they are already taking in this direction, particularly the self-regulatory principles issued by the DMA and other trade associations in July and the development of an icon-based notice regime being developed by the Future of Privacy Forum.

Moreover, industry representatives stressed that the provision of notice and choice is more effective than legislation or regulation in meeting consumer needs because privacy is a subjective value; some consumers may be willing to relinquish data in exchange for certain things, such as targeted offers, while others are not. Because it is extremely difficult to determine what choices consumers will actually make in any particular context, the industry representatives argued that the government should not attempt to

dictate a one-size-fits-all choice on behalf of them. Moreover, the government's attempt to "protect" privacy in such a way would impose significant costs in the form of stifled innovation and the reduction of funding for online content that is now offered to consumers for free.

**What's the harm?**

As mentioned above, the commission has also relied on a harm-based approach to privacy, bringing enforcement actions when consumers have suffered tangible harm. Apart from saying that this approach has not been as successful as the commission would like, Chairman Leibowitz did not directly address the question of what harms arise in the privacy context and whether they should be actionable.

Comments from BCP Director Vladeck suggest, however, that the commission may be moving away from only exercising its authority against tangible harms. In earlier interviews, he has taken the position that privacy-related harm can occur without tangible injury. Specifically, he has said that "harm" includes not just tangible injury, such as monetary loss, but also intangible harms such as "dignity violations." Former BCP Director Howard Beales noted that there is nothing in the commission's harm-based approach that says that harm must be tangible to be actionable, but he cautioned that the harms must be real and articulated. He also stressed that the government must find the most effective and least costly way to avoid the harms it identifies.

Consumer advocates expressed their agreement with Director Vladeck's thinking, saying, for example, that anonymity is an important social value and that consumers have the right to know what data is collected about them and how they are categorized based on the data. In its written comments to the roundtable, the Center for Democracy and Technology took this a step further by urging the commission to affirm that a violation of any one of the FIPs results in individual harm and to use the FTC's unfairness authority under Section 5 of the FTC Act to pursue such violations. If

the CDT's recommendation were to become a reality, a company could face liability for, for instance, "harming" consumers by collecting even one element of data that is more than that "relevant" or "necessary to accomplish a specified purpose" (i.e., violation of the "data minimization" principle).

#### What's next?

As discussed above, Chairman Leibowitz acknowledged the limitations of the commission's notice-and-choice and harm-based approaches to privacy. He said that the commission is open to new approaches and that, over the next six months, it will be working to figure out the best approach. He did not express an inclination toward one approach or another.

In his remarks closing the roundtable, BCP Director Vladeck echoed the chairman but also gave a hint that his views may be leaning toward regulation. He stated that consumers do not really understand privacy and that consumer disclosure as we currently know it does not work. He gave a nod to companies that are giving consumers better tools to learn about tracking. At the same time, he noted that few consumers use them and wondered whether consumers are making bad decisions even when they understand the harms. If the commission's approach is shaped by this theory—e.g., in the form of a trade regulation rule—it will signify a drastic shift away from giving consumers the information they need to make their own choices to the government's making choices for them.

#### Related news

##### The Federal Trade Commission Improvements Act

In related news, the FTC Improvements Act passed the House of Representatives on December 11, 2009, on a vote of 223–202. If it passes the Senate in its current form, the bill will give the commission substantially more power. Specifically, the bill would:

*See, FTC roundtable, page 24*

## In the Privacy Tracker this month...

### Looking back, looking ahead

This month on the Privacy Tracker Web site subscribers have exclusive access to a collaborative article that forecasts the privacy landscape for the year ahead. Experts provide sector-specific privacy forecasts for 2010.



In addition, the audio archive of the January Privacy Tracker call is now available. The call features a dynamic conversation that looks back at 2009 privacy legislation in 2009 and looks ahead to 2010.

Privacy Tracker keeps you up-to-date on all federal and state privacy legislation with monthly interactive audio conferences where you can request specific coverage, weekly e-mails, and a Web dashboard of timely articles and reports. **Privacy is the hot bipartisan issue for 2010**—subscribe today to keep up with the latest developments affecting your business.

*Try it before you buy it! E-mail us to get a free week-long demo subscription to the Privacy Tracker. [privacytracker@privacyassociation.org](mailto:privacytracker@privacyassociation.org).*

[www.privacytracker.org](http://www.privacytracker.org)



## The Lighter Side of Privacy



Reprinted with permission from Slane Cartoons Limited.

**FTC roundtable**

*continued from page 23*

- permit the commission to impose civil penalties for violations of Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices (currently, it can seek only equitable relief);
- give the commission Administrative Procedures Act rulemaking authority, which is far more flexible than its current rulemaking authority under the Magnuson-Moss Act; and
- expressly permit the commission to pursue cases of secondary liability (i.e., where a person has provided substantial assistance to another who has violated a law enforced by the commission).

It is not yet clear how the Senate will react. The bill has to move through the Banking Committee (the FTC provisions are just part the Wall Street Reform and Consumer Protection Act), but Senators

on the Commerce Committee may also be trying for a seat at the table before the bill goes to the Senate floor—something Banking Committee members may resist. Democrats on the Senate Commerce Committee may be more inclined to support the extension of FTC authority than those on the Banking Committee, which does not have jurisdiction over the FTC.

The bill faces substantive hurdles in addition to the jurisdictional ones described above. Some Democrats are uncomfortable with the underlying bill itself, and, of course, many Republicans are uncomfortable with not only the creation of an entirely new agency—the CFPA, which would be created by the Wall Street Reform and Consumer Protection Act—but also such sweeping new powers being granted to an existing agency (the FTC). There are so many moving pieces that it’s difficult to predict the provisions’ chances. In addition, with healthcare reform consuming so much of the Senate’s energy, few expect resolution soon. Nevertheless, this is a very

important bill to watch, given the powers it would confer on the FTC.

*The final roundtable takes place on March 17 in Washington, DC.*

*D. Reed Freeman, Jr., CIPP, is a partner in Morrison & Foerster’s Privacy and Data Security Group. He focuses on all aspects of consumer protection law, including privacy, data security, and breach notification, online and offline advertising, and direct marketing.*

*Julie O’Neill, of counsel in the Washington DC office of Morrison & Foerster, counsels clients in all areas of state and federal consumer protection law. Ms. O’Neill previously served as a staff attorney in the FTC’s New York regional office, where she investigated violations of federal antitrust and consumer protection law.*

## NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION

# REALLY? AN ORGANIZATION DEDICATED TO PROPER INFORMATION DESTRUCTION?



**You bet - and for good reason!** Improperly discarded paper and electronic records are among the most overlooked and vulnerable areas of information protection. Information destruction has also become an area of increasing regulation, enforcement actions and fines.

Since 1994, the National Association for Information Destruction (NAID) has been the leading proponent of standards development and education related to proper information disposal and increase employee compliance.

NAID’s 1,000-plus service providers around the world are dedicated to helping organizations make informed decisions on records destruction, vendor selection, employee training, and contract language and policy development.



Get serious about information disposal - [www.naidonline.org](http://www.naidonline.org)





IBM and the IBM logo are registered trademarks of International Business Machines Corporation in the United States and/or other countries. Other company, product and service names may be trademarks or service marks of others. ©2008 IBM Corporation. All rights reserved. P21905

A black and white photograph of three business professionals in a meeting. A man on the left is looking towards a woman in the center, who is looking towards a man on the right. They are all dressed in business attire. The background shows a modern office setting with a whiteboard and a window.

# YOU CAN ENHANCE YOUR RESPONSIVENESS

Governments at all levels face difficult challenges. Economic slowdown. High expectations from key constituents – citizens, businesses, suppliers, employees and other agencies. Escalating costs and budget shortfalls. Security issues. How do you respond? How do you transform the way you work?

Enter IBM. With a unique combination of privacy and data protection experience, business insight and end-to-end solutions, IBM can help your business succeed. Innovate. Grow. Respond in real time. Prepare for tomorrow. You're ready to differentiate your business.

IBM holds more security and privacy copyrights and patents than any other company. We know what we are doing...now you know too. Why go anywhere else? To learn more about IBM Global Business Services Public Sector's Security, Privacy, Wireless, & IT Governance offerings, email us at [SecPrivW@us.ibm.com](mailto:SecPrivW@us.ibm.com).

## Global Privacy Dispatches



### Global Privacy Dispatches

#### CANADA

By John Jager, CIPP/C

#### A look at Bill 54

During the past years, a number of Canadian privacy laws have been undergoing statutory review. A review of the federal Personal Information Protection and Electronic Documents Act



John Jager

(PIPEDA) commenced in the fall of 2006, a review of the Alberta Personal Information Protection Act (AB PIPA) commenced in 2007 and a review of the British Columbia Personal Information Protection Act (BC PIPA) began in 2008.

While all of these reviews have resulted in committee reports to the respective legislatures, only the government of Alberta has tabled a bill to amend its private-sector privacy legislation. On October 27, 2009, the government of Alberta introduced Bill 54—Personal Information Protection Amendment Act, 2009.

The bill contains an extensive number of amendments. This dispatch focuses on some key issues that will impact private-sector organizations going forward.

#### Breach notification:

Bill 54 creates a statutory requirement for notification when personal information (PI) is lost or has been subject to unauthorized access or disclosure. Rather than creating a mandatory requirement for organizations to notify affected parties, Bill 54 requires that organizations having PI under their control must, without unreasonable delay, provide notice to the privacy commissioner of any incident involving the loss of or unauthorized access to or disclosure of the PI, where a

reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

If an organization suffers a loss of or unauthorized access to or disclosure of PI where the organization would be required to provide notice to the privacy commissioner, the commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure. The notification to affected individuals would have to be in a form and manner as prescribed by the regulations, and within a time period determined by the commissioner. Under the bill, the commissioner must establish an expedited process for determining whether to require an organization to notify individuals in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

#### Access requests:

Bill 54 includes a number of amendments to the sections relating to access and correction, and includes a number of clarifications and the reorganization of some sections. On the matter of fees, Bill 54 proposes that organizations may not charge a fee in respect of a request for personal employee information. Section 33, which requires organizations to make reasonable efforts to ensure that PI is accurate and complete, is amended by adding the words “to the extent that is reasonable for the organization’s purposes in collecting, using, or disclosing the information.”

*“The notifications must be made at or before the collection or transfer, in writing or orally...”*

#### Employee personal information:

Currently PIPA permits the collection, use, and disclosure of personal information of employees and prospective employees if the information is to be used for a purpose that is reasonable and related to an employment relationship. Bill 54 amends these relevant sections to extend the collection, use, and disclosure of employee personal information to the management of the post-employment relationship.

#### Privacy notice:

Bill 54 adds a new section which deals with notification requirements respecting service providers outside Canada. Organizations using foreign service providers to collect PI with the consent of an individual must notify the individual of that collection. If the organization transfers PI, directly or indirectly, to a service provider outside Canada, individuals must be so notified. The notifications must be made at or before the collection or transfer, in writing or orally, and must include how individuals can obtain access to written information about the organization’s policies and practices with respect to service providers outside Canada. The notification must also include the name or title of a person who is able to answer, on behalf of the organization, an individual’s questions.

A copy of Bill 54 is available at the Alberta government Web site, or at the following URL: [www.assembly.ab.ca/ISYS/LADDAR\\_files/docs/bills/bill/legislature\\_27/session\\_2/20090210\\_bill-054.pdf](http://www.assembly.ab.ca/ISYS/LADDAR_files/docs/bills/bill/legislature_27/session_2/20090210_bill-054.pdf).

*John Jager, CIPP/C, is vice president of research services at Nymity, Inc., which offers Web-based privacy support to help organizations control their privacy risk. He can be reached at john.jager@nymity.com.*

## FRANCE

By Pascale Gelly

### CNIL sanction procedure overruled by the Court of Appeal

In late 2006, the French data protection authority issued a 30,000 euro sanction against Inter Confort for improper handling of objection requests to direct marketing via telephone. The sanction followed the CNIL's onsite investigation of Inter Confort. Inter Confort challenged this sanction decision before the Court of Appeal (Conseil d'Etat) on procedural grounds. The onsite investigation procedural rules set forth by the Data Protection Act and its implementation decree provide extensive powers to the authority to access private premises, even outside of business hours, without prior warning and without the data controller being present. These powers being almost limitless, the court considered that it was essential "for proportionality purposes" to counterbalance them by putting them under the control of a judge of the judiciary system. The court considers this to be achieved by the DP Act insofar as it gives the right to the data controller to object to the investigation, in which case the investigation can occur only with the prior authorization of a judge. As defendants must be made aware of their rights, the Appeal Court cancelled the CNIL decision because the authority failed to inform the data controller of its right to object to the investigation.



Pascale Gelly

### French senators pursue their goal for an "enhanced" Data Protection Act

Following their report, Privacy in the Era of Digital Memory: For an Increased Trust Between Citizens and The Information Society, two senators filed a bill on November 10 to modify the French Data Protection Act.

*"The CNIL announced that it had conducted onsite investigations at two major customer call centres."*

The bill intends to introduce several changes to the law, including requirements such as:

- mandatory installation of a data protection officer for organizations with more than 50 employees;
- an obligation to notify the CNIL of data security breaches;
- an obligation for organizations' Web sites to enable individuals to exercise their data protection rights online;
- changing the existing right of objection to a right of deletion;
- changing the content of privacy notices to specify the data retention limit;
- publicizing the hearings of the CNIL litigation committee;
- increasing CNIL sanction powers to include fines of up to 300,000 euros and the option to publicize the sanctions, even against a "good faith" infringer, so that the CNIL enforcement powers will be more efficient.

The senators are also joining the efforts of the French Secretary of State for the digital economy to work on a "droit à l'oubli"—a sort of right "to oblivion" or, some would say right "to deletion," a French cousin to the right "to be left alone." At a November conference at SciencesPo, CNIL President Alex Türk disclosed very personal information about his youth and recruiters presented a code of conduct.

[www.senat.fr/dossierleg/ppl09-093.html](http://www.senat.fr/dossierleg/ppl09-093.html)

### Calling on call centres

The CNIL announced in mid-November that it had conducted onsite investigations at two major customer call centres.

The main check was on the security

and confidentiality of customer data collected and processed by the call centres. An area of improvement was identified: the need for action logs e.g., who accessed what, who modified what and when, etc...

Employee-monitoring tools were also investigated. More onsite "calls" are expected.

[www.cnil.fr/la-cnil/actu-cnil/article/article/2/les-centres-dappel-sous-controle/#](http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/les-centres-dappel-sous-controle/#)

*Pascale Gelly of the French law firm Cabinet Gelly can be reached at [pg@pascalegelly.com](mailto:pg@pascalegelly.com).*

## GERMANY

By Flemming Moos

### The privacy work programme of the new German Federal Government

The newly elected German government has set out in a coalition agreement how it intends to govern during the next four years. Remarkably, the 124-page document contains a specific chapter on privacy issues. The privacy work programme of the new government focuses on the following issues:



Flemming Moos

- The law that would allow German intelligence agencies to engage in online surveillance of private computers will remain. However, the "protection of the core area of private lifestyles," shall be improved. The coalition will await a ruling by the Constitutional Court on the retention of data before allowing intelligence agencies to access telecommunications companies' data on their customers' call details.

See, *Global Privacy Dispatches*, page 28

*Global Privacy Dispatches*

*continued from page 27*

- The government wants to better protect employees from their employers spying on them. Employers will be allowed to use only data that affects the employer-employee relationship. The government intends to add to the federal German Data Protection Act (BDSG) a new chapter on employee privacy.
- Even more, the government strives at an overall modernization of the BDSG. It is intended to make the law more readable and technology-neutral; also the framework for clear and unambiguous declarations of consent by individuals shall be improved and existing information obligations shall be expanded. In performing this task, the government also wants to examine whether changes can be made with a view to eliminating superfluous red tape.
- Also, the issue of sharing financial data with the U.S. seems to be under further scrutiny. The coalition agreement says any SWIFT agreement should have a "high level of data protection" and should only be used for the purpose for which it was requested.
- The government wants to make greater use of biometric procedures (passports, identity cards, visas, residence permits) and amend the Act Governing Passports and Identity

*"The creation of a foundation on data privacy is planned. The foundation will test and certify services and products with respect to data protection law compliance..."*

Cards to this end while maintaining data protection.

- The creation a "foundation on data privacy" is planned. The foundation will test and certify services and products with respect to data protection law compliance and adherence to the principles of data avoidance and data economy.

**Decision of the Federal Court of Justice: opt-out consent to postal advertising**

On November 11, 2009, the German Federal Court of Justice handed down a judgment on the privacy aspects of the "HappyDigits" bonus programme. The court held that an opt-out consent by participants relating to postal advertising that was included in the registration form for the programme is compliant with applicable German data protection law provisions. In this respect, the court applied Sec. 4 of the BDSG, according to which consent also can be given simultaneously with other declarations (here, the participation in the bonus programme) in case special prominence is given to the declaration of consent (e.g. by printing in bold). Interestingly, the court also stated clearly that, in this respect, the September 1, 2009 amendment of the BDSG has not brought about any changes to the law. Rather, also the recently introduced Sec. 28 paragraph 3a BDSG shall provide for a respective opt-out solution. It must be borne in mind however, that this is only true for postal advertising. With respect to advertising via telephone, telefax, e-mail, or other electronic means, an opt-in consent is generally required under German law, as the Federal Court of Justice had earlier declared in its ruling dated July 16, 2008 on the "Payback" bonus programme.

**DPA of Berlin: strict approach to denied person screenings**

As already reported in the October Issue of the *Privacy Advisor*, the Düsseldorf Kreis adopted a resolution on privacy aspects of employee screenings in April 2009, following a moderate

*"It seems doubtful whether this approach is in fact in line with the findings and the resolution of the Düsseldorf Kreis."*

approach what concerns the overall permissibility of such screenings. The DPA of Berlin apparently applies a much stricter approach; according to an informative letter to other German DPAs dated August 31, 2009, he is of the opinion that even a usage of the denied persons lists included in the EU Regulations 2580/2001 and 881/2002 (which are *per se* binding in Germany) cannot be justified under German data protection law provisions. In particular, the Data Privacy Officer of Berlin criticizes that the provisions of these EU Regulations are too broad to qualify for a statutory provision that would allow the usage of the data for screening purposes. Moreover, he takes the view that the balancing of interest test is in favour of the affected individuals because the lists seem to be outdated and erroneous and in fact the companies would not face any relevant sanctions for non-compliance with the applicable EU Regulations. It seems doubtful whether this approach is in fact in line with the findings and the resolution of the Düsseldorf Kreis. Anyhow, it is recommendable for German businesses to consult with the competent DPA before introducing a denied person screening system in Germany.

*Flemming Moos is an attorney at DLA Piper and the chair of the IAPP KnowledgeNet in Hamburg, Germany. He is a certified specialist for information technology law and a former member of the IAPP Publications Advisory Board. He can be reached at [flemming.moos@dlapiper.com](mailto:flemming.moos@dlapiper.com).*

## Calendar of Events

### FEBRUARY

**4** **Université AFCDP des Correspondants Informatique & Libertés**  
Paris, France  
[www.afcdp.net](http://www.afcdp.net)

**11** **IAPP KnowledgeNet – Paris**

**16** **IAPP KnowledgeNet – Hamburg**

**24** **IAPP Certification Testing – Columbus, OH**

**24** **IAPP Certification Testing – New York, NY**

**24** **IAPP Certification Testing – Victoria, BC**

**26** **IAPP Certification Testing – St. Paul, MN**

### MARCH

**16** **IAPP Tenth Anniversary Celebration**  
Washington, DC/Various other

locations via telecast  
[www.privacyassociation.org](http://www.privacyassociation.org)

**17** **FTC Privacy Roundtable**  
FTC Conference Center  
Washington, DC

### APRIL

**19-21** **IAPP Global Privacy Summit**  
Washington, DC  
[www.privacysummit.org](http://www.privacysummit.org)

**21** **IAPP Certification Testing – Washington, DC**

### MAY

**2-8** **APPA Privacy Awareness Week**  
[www.privacyawarenessweek.org](http://www.privacyawarenessweek.org)

**26-28** **IAPP Canada Privacy Symposium 2010**  
Toronto, ON

### JUNE

**14-15** **IAPP Practical Privacy Series**  
Santa Clara, California

### SEPTEMBER

**29-1** **IAPP Privacy Academy**  
Baltimore, MD  
[www.privacyacademy.org](http://www.privacyacademy.org)

**30** **Privacy Dinner**  
Baltimore, MD  
[www.privacyassociation.org](http://www.privacyassociation.org)

### OCTOBER

**27-29** **32nd International Conference of Data Protection and Privacy Commissioners**  
Jerusalem, Israel

### DECEMBER

**7-8** **IAPP Practical Privacy Series**  
Washington, DC  
[www.privacyassociation.org](http://www.privacyassociation.org)

*To list your privacy event in the Privacy Advisor, e-mail Tracey Bentley at [tracey@privacyassociation.org](mailto:tracey@privacyassociation.org)*

## Privacy News

### European legislative update

Linklaters has released its 2009/2010 edition of Linklaters' Data Protected, a summary of European data protection legislation. The updated report includes reviews of data protection legislation in all Member States, European Economic Area States (Iceland, Liechtenstein, and Norway), and Switzerland and Russia.

The update reflects major changes to data protection laws in Germany, and new content including questions on the formal requirements for consent and Linklaters' proposals for the reform of the Data Protection Directive.

[www.linklaters.com/pdfs/extranet/DataProtected/2009\\_2010.pdf](http://www.linklaters.com/pdfs/extranet/DataProtected/2009_2010.pdf)

### ONC names privacy, security workgroup members

The Office of the National Coordinator for Health IT named 17 to the Health IT Policy Committee privacy and security workgroup in December.

#### The members are as follows:

- Deven McGraw, Chair, Center for Democracy & Technology
- Rachel Block, Co-Chair, NYS Department of Health
- Paul Tang, Palo Alto Medical Foundation
- Latanya Sweeney, Carnegie Mellon University
- Gayle Harrell, Consumer Representative/Florida
- Mike Klag, Johns Hopkins University, Public Health
- Judy Faulkner, Epic, Inc.
- Paul Egerman, Consultant
- Dixie Baker, SAIC
- Paul Uhrig, SureScripts
- Terri Shaw, Children's Partnership
- John Houston, University of Pittsburgh Medical Center
- Joyce DuBow, AARP
- A. John Blair, MD, Provider
- Peter Basch, MD, Provider
- Justine Handelman, Blue Cross Blue Shield
- Dave Wanser, National Data Infrastructure Improvement Consortium
- Kathleen Connor, Microsoft

# SURVEILLED

Scenes from the IAPP Practical Privacy Series in Washington, DC.

*Privacy pros gathered at the Willard InterContinental Hotel for the two-day Practical Privacy Series event in early December. Day one explored the role of the Federal Trade Commission in consumer privacy protection. Day two focused on new dimensions in government privacy: cookies, clouds, and collaborative computing.*



*Left: FTC Bureau of Consumer Protection Director David Vladeck (left) opened the day-one event "The Role of the FTC in Consumer Privacy Protection." Bob Belair of Oldaker Belair & Wittie LLP listens.*



*Top: On day two, attendees explored new dimensions in government privacy. Greg Dupier of Booz Allen Hamilton, Lewis Oleinick of the Defense Logistics Agency, Peter Fleischer of Google, and consultant Robert Gellman lead the session "Perspectives on Cloud Computing."*

*Right: Robert Clark (standing), the oversight and compliance officer for the Office of DHS Assistant Secretary for Cybersecurity and Communications elicits a laugh from Rick Aldrich, a Booz Allen Hamilton contractor, during the session "Banners, Notices and MOAs: What the National Cybersecurity Strategy Means for Your Agency."*



*Despite wet weather and trying travel conditions, the room was full.*

## Privacy News

### New IAPP Europe Board members

The IAPP has announced new members for its European Advisory Board. Privacy experts from a variety of government and industry sectors will help inform the expansion of IAPP Europe, which was launched in November to provide tailored education, networking, and certification opportunities for European data protection professionals.

#### New IAPP Europe board members

- Bojana Bellamy, Director of Data Privacy, Accenture
- Ruth Boardman, Partner, Bird & Bird
- Gary Davis, Deputy Commissioner, Office of the Data Protection Commissioner, Ireland
- Rafael Garcia Gozalo, Head of the International Department, Spanish Data Protection Authority
- Pascale Gelly, Cabinet Gelly, AFCDP Board Member
- Sue Gold, Executive Counsel, The Walt Disney Company Limited
- Christoph Klug, Managing Director, German Association for Data Protection and Data Security (GDD)
- Gabriela Krader, Data Protection Officer, Deutsche Post
- Christopher Kuner, Partner, Hunton & Williams
- Denise Lebeau-Marianna, Partner - Avocat à la cour, ITC Department, Baker & McKenzie SCP
- Xavier Leclerc, Vice President AFCDP, Managing Director Axil-Consultants
- Neil Matthews, UK Privacy Officer, Acxiom Limited
- Rocco Panetta, Partner, Panetta & Associati – Studio Legale
- Florence Raynal, Head of International and European Affairs of the CNIL
- David Smith, Deputy Commissioner, Information Commissioner's Office, United Kingdom
- Toby Stevens, Director, Enterprise Privacy Group
- Florian Thoma, Chief Data Protection Officer, Siemens
- Richard Thomas CBE LLD, Centre for Information Policy Leadership, Hunton & Williams LLP
- Henriette ("Jetty") Tielemans, Partner, Co-Chair of the Global Privacy and Data Security Group, Covington & Burling LLP
- Bridget Treacy, Partner, Hunton & Williams
- Eduardo Ustaran, Partner and Head of the Privacy and Information Law Group, Field Fisher Waterhouse LLP

## Congratulations, Certified Professionals!

*The IAPP is pleased to announce the latest graduates of our privacy certification programs. The following individuals successfully completed IAPP privacy certification examinations held in fall and winter 2009.*



John Patrick Ahern, CIPP/G  
Lalit Kumar Ahluwalia, CIPP  
Ann Allinson, CIPP  
Joan Susan Antokol, CIPP  
Julian Appel, CIPP/IT  
Jennifer Carroll Archie, CIPP  
Asif Arman, CIPP  
Brian W. Arney, CIPP/IT  
Wayne Joseph Bate, CIPP/C  
Essie Louise Bell, CIPP/G  
Kevin Charles Boyle, CIPP  
Margaret Kathleen Bramwell, CIPP  
Jane L. Braun, CIPP/IT  
William B. Brinkley, CIPP/G  
Mark A. Brown, CIPP/G  
Pamela S. Bruce, CIPP  
James Lesley Bryant, CIPP  
Gerald Burton, CIPP/G  
Edward Allen Byrd, CIPP  
Sang Kyung Byun, CIPP  
Colin Alexander Campbell, CIPP/IT  
Kerey L. Carter, CIPP/G  
Debra Marie Castanon, CIPP/IT  
Ruben D. Chacon, CIPP  
Darren Curtis Chin, CIPP/C

Mithin Jay Chintaram, CIPP  
Christopher Joel Clancy, CIPP  
Patrick Michael Clary, CIPP  
Maureen Ann Clements, CIPP  
Kelly Hugh Cook, CIPP/G  
Brett Joseph Croker, CIPP  
Laquawn M. Curry, CIPP/G  
Ania Magdalena Czynielewska, CIPP  
Lina D'Aversa, CIPP/C  
Lashaunne Graves David, CIPP/G  
Daryl Edward Davis, CIPP/G  
Helene Demoulin, CIPP/IT  
Sophie Dessalle, CIPP  
Marsha L. Devine, CIPP/G  
Roderick Wayne Duff, CIPP/G  
Jacquelyn Louise Dutcher, CIPP  
Joanne Easdow, CIPP/C  
Kristen Marie Ellis, CIPP/G  
James Vincent Episcopio, CIPP  
Anthony C. Escobedo, CIPP/G  
Brian DuPerre, Esq., CIPP  
Traci Lynne Ewers, CIPP/G  
Kelly Frances Farmer, CIPP  
Meghan Kathleen Farmer, CIPP/G  
Michael Joseph Ferguson, CIPP/C

LeRoy Elliot Foster, CIPP/IT  
Stephen Todd Fraley, CIPP  
Marc Gagne, CIPP/C  
Ronald Paul Gandy, CIPP  
Cheri Gatland-Lightner, CIPP/G  
Kathryn Gillia, CIPP  
Scott Matthew Giordano, CIPP/IT  
Mark Henry Goldstein, CIPP  
John G. Goodson, CIPP/G  
Connie Ann Graham, CIPP  
Philip McKinley Greene, CIPP/IT  
William Edward Growney, CIPP  
Wayne Lee Gustafson, CIPP  
Sheila A. Guthrie, CIPP/C  
Cynthia Ann Gutz, CIPP  
Brian Douglas Hall, CIPP  
Mindy Ayn Harbeson, CIPP  
Mary Louise Harter, CIPP/IT  
Tammy A. Hastie, CIPP/C  
Sari Lyn Heller Ratican, CIPP  
Jacob J. Herstek, CIPP  
Gregory Robert Hewes, CIPP/IT  
Elizabeth Susan Hidaka, CIPP  
Travis James Hildebrand, CIPP/G  
Georges Houde, CIPP/IT

*Periodically, the IAPP publishes the names of graduates from our various privacy credentialing programs. While we make every effort to ensure the currency and accuracy of such lists, we cannot guarantee that your name will appear in an issue the very same month (or month after) you officially became certified.*

*If you are a recent CIPP, CIPP/G or CIPP/C graduate but do not see your name listed above then you can expect to be listed in a future issue of the Advisor. Thank you for participating in IAPP privacy certification!*



Gretchen Kreller Hiley, CIPP  
 Carolyn Cunnold Holcomb, CIPP  
 Gail A. Horlick, CIPP/G  
 Amy J. Howe, CIPP/G  
 Max Montgomery Howie, CIPP/G  
 Alan Andrew Isham, CIPP/IT  
 Keith Alan Jantzen, CIPP  
 Carol Anne Jaques, CIPP/C  
 Myrl B. Jowell, CIPP/G  
 Albert King, CIPP/G  
 Catherine Sansum Kirkman, CIPP/G  
 Felicia P. Kittles, CIPP/G  
 David H. Knowles, CIPP/G  
 Vava Kolinski, CIPP/C  
 Linda Komperda, CIPP  
 Andrew Brian Lachman, CIPP/G  
 James Lai, CIPP  
 James Michael Laskowski, CIPP  
 Gigi Waitz Leung, CIPP/IT  
 Greg Levine, CIPP/G  
 Thomas P. Levis, CIPP  
 Ryan Kyle Liu, CIPP  
 Marc S. Loewenthal, CIPP  
 Kenneth W. Long, CIPP/G  
 Raymond Lopez, CIPP  
 Elena Antoinette Lovoy, CIPP/C  
 Victor A. Loy, CIPP/IT  
 Kevin Lyday, CIPP/G  
 John David Macias, CIPP/G  
 Thomas Patrick Madden, CIPP/G  
 Kelly Marie Matoney, CIPP/G  
 Lester Masao Mayeda, CIPP/IT  
 Matthew David McAllister, CIPP  
 Brian McKay, CIPP  
 Sam D. Monasteri, CIPP/IT  
 Carlos Mondesir, CIPP/C  
 Robert James Morgan, CIPP  
 Timothy W. Morrison, CIPP  
 Mehmet Munur, CIPP  
 Polly J. Nelson, CIPP  
 Julie Hua Ni, CIPP  
 Brian Christopher Nicholson, CIPP/G  
 Jennifer Nikolaisen, CIPP/G  
 Victoria Barbara Ocholla, CIPP  
 Charles R. Offer, CIPP/IT

Michael Robert Overly, CIPP  
 Sylvia Ortega, CIPP  
 Ray Pathak, CIPP/C  
 James David Pearson, CIPP/G  
 Cecil Francis Pineda, CIPP  
 Claudiu Popa, CIPP  
 Karen C. Powell, CIPP  
 Marion A. Reeves, CIPP/G  
 Jeanne Marie Robinson, CIPP  
 Michele L. Robinson, CIPP  
 Susan Loraine Rohland, CIPP/C  
 Nicole Marie Rosen, CIPP/IT  
 Glenn Ross, CIPP/C  
 K Roal, CIPP  
 Anita L. Sandmann-Hill, CIPP/G  
 Carla Scher, CIPP/IT  
 Vineet R. Shahani, CIPP  
 Ramachandra Kudgi Shenoy, CIPP  
 Inamullah Siddiqui, CIPP  
 Ryan Thomas Smyth, CIPP  
 David Michael Sutton, CIPP/C  
 Angela Swan, CIPP/IT  
 Gray E. Terry, CIPP  
 Elliott Caleb Tomes, CIPP/G  
 Katharine Tomko, CIPP  
 Robert Thomas Traver, CIPP/IT  
 Sherri Trip, CIPP/IT  
 John Laurence Trotti, CIPP  
 William A. Turner, CIPP/C  
 Mary E. Vansickle, CIPP/C  
 Ralph S. Vaughn, CIPP/G  
 Danny Lamonte Wade, CIPP/G  
 Carol Elaine Waller, CIPP/G  
 Jacquay D. Waller, CIPP/G  
 Terry Wang, CIPP/G  
 Douglas Keith West, CIPP/G  
 Laurene West, CIPP  
 Jeff Wilson, CIPP  
 Alexander Windel, CIPP/IT  
 Jeffrey Yarges, CIPP  
 Clark Kiyoshi Yogi, CIPP/IT  
 Sabiha Gulshan Zafar, CIPP/G  
 Paola Zeni, CIPP

## PRIVACY PREDICTIONS -2010-

Businesses will continue to push for new technologies such as “cloud computing” and increasing use of mobile technologies, which will put pressure on privacy professionals to understand the implications of these new and rapidly evolving technologies. Business will continue to grapple with the implications of social networking applications as they relate to privacy and by the end of 2010 there will be first-generation products on the marketplace focused on helping business monitor and control such products. Regulation will continue to become more complex and prescriptive in an attempt to address privacy breaches. The accountability for privacy in situations where a process has been outsourced/off-shored will come under scrutiny in 2010 as the result of a major breach somewhere in the world. The U.S. will move closer to a national privacy/data security law, but will fail to obtain a federal DPA.

—Jeff Green, CIPP/C,  
 Vice President, Global  
 Compliance & Chief Privacy  
 Officer, RBC

# PRIVACY PREDICTIONS -2010-

## Privacy and data protection in Australia and New Zealand, 2010

Legislation to implement substantial proportions of the ALRC report on privacy, as set out in the Federal Government Response of October 2009, will be introduced into Parliament in the first half of 2010 but may not be passed before the next federal election, delaying its final enactment until 2011. The federal government will announce its response to the remainder of the ALRC report after the federal election, likely to be held in the second half of 2010. Significant progress will be made in introducing electronic health identifiers for all Australians and providing them with additional legal protection. A number of initiatives to connect electronic health information for clinical purposes will emerge, connecting the significant repositories already developing in individual hospitals and medical practices. The New Zealand Law Commission will make significant progress with its inquiry into privacy law in New Zealand. Banking and other sectors of the economy will make a significant push into mobile transactions. The iappANZ will hold another highly successful annual conference later in the year.

*Malcolm Crompton, CIPP,  
Managing Director, Information  
Integrity Solutions P/L*

## 10 New Year's privacy resolutions

*By Luis Salazar, CIPP, and Jorge Rey*

*A group of South Florida IAPP members braved the winter elements—blue skies, sunshine, warm temperatures—to attend a KnowledgeNet meeting in Miami in December. Jorge Rey led the interactive session on the apropos topic: Privacy Resolutions.*

*Although attendees represented a wide range of industries—pharma, banking, education, professional services, and more—all shared remarkably similar concerns and goals. Here are their top resolutions (in reverse order).*

### 10. Perform internal/external penetration and social engineering testing

No matter the industry, all participants agreed that “knowing” is a critical part of the privacy battle. And while IT security weaknesses remain critical, good-old fashioned social engineering is a major concern, especially in these difficult financial times. Rey, in particular, advised that simply testing employees and testing their compliance with security measures is critical. Will the help desk release passwords? Will a receptionist divulge critical employee names?

“People can violate privacy protocols just because they are eager to help and be service-oriented,” offered Linda Clark, CIPP, and director and senior corporate counsel at LexisNexis. “We teach employees to be aware of social engineering and provide guidance on how to respond in certain situations—something like ‘at

Lexis we value privacy, and I can't disclose the information that you are asking for'—to help them comfortably and politely refuse such requests.”

### 9. Assess and update legal agreements and vendor due-diligence procedures

Like losing weight or eating right, this is one of those resolutions that everyone undertakes each year, but often finds nearly impossible to actually carry out to the level they would like. Odelin Fernandez, Jr. (Odie to his friends), who manages the vendor program as operations and technology risk supervisor at Mercantil Commercebank, noted that “making sure vendors' contracts are up-to-date on changing requirements, auditing vendor requirements, plus conducting due diligence on potential vendors is time consuming and often frustrating, but it's an absolutely essential compliance step. So often, vendors are the weak link.”

### 8. Assess and update marketing programs to maintain privacy compliance

Two concerns drove this resolution: the evolving nature of behavioral marketing and the need to limit data intake. CAN-SPAM, behavioral marketing, and even the revised product endorsement guidelines concern South Florida privacy professionals. But for David Vance, senior director and compliance counsel for Noven Pharmaceuticals, avoiding unwanted data intake is critical.

“Noven does promote some prescription products direct to customers,” said Vance. “And even inadvertent intake of information can potentially subject the company to healthcare privacy laws and regulations. So, like other pharmaceutical companies, we maintain safeguards against consumers sending us personal medical information—even when we don't ask for it. We also make sure that vendors that must use some personal medical information to administer patient assistance programs or co-pay voucher programs, do not share that



Luis Salazar



Jorge Rey

*“Auditing and spot-checking are indispensable methods of making sure that vendors are in compliance. All attendees resolved to make this one of their top tasks for 2010.”*

information with us. If a consumer wants to report an apparent adverse event, however, we of course take that very seriously.”

#### **7. Hire information security and/or privacy professionals**

It should come as no surprise given the current economic climate that all of the meeting’s participants are running very lean privacy programs. Yet many are tasked with handling a wider variety of responsibilities than they have in the past. “Everyone is happy to be employed these days, but it is equally important to have the right people in the right position,” noted one.

Thus this key resolution: Hire the right personnel to address critical problems. Perhaps an unspoken resolution is needed: Get more money and resources for privacy.

#### **6. Perform a privacy and/or information security compliance due diligence for current vendors**

Sure, vendors sign contracts agreeing to comply with privacy laws and procedures, but are they really doing it? One attendee voiced a common concern: “Too often it seems as if vendors will say and agree to anything to get the business, but actual execution is another thing.”

Auditing and spot-checking are indispensable methods of making sure that vendors are in compliance. All attendees resolved to make this one of their top tasks for 2010.

#### **5. Perform internal privacy and information security compliance audits**

Measuring performance is crucial to managing it, and privacy is no different. All participants agreed that living up to this resolution requires covering some audit basics, namely “what’s in scope, what’s not?”

But at perhaps the other extreme, simply creating some “self-checklists” to educate employees and raise privacy awareness is remarkably effective,” noted Todd Sussman, privacy officer for the Broward County Florida Public School System.

#### **4. Implement technologies to prevent data leakage**

If it weren’t for budget constraints, this resolution would probably top the list. Be it e-mail encryption, electronic shredding, or data-leakage software, rolling out robust technology is something every privacy professional wants to do.

#### **3. Develop specialized privacy and/or information security training**

Like learning a new language or traveling abroad, this is another one of those resolutions that everyone makes but often struggles to carry out. Attendees noted resource constraints, especially, as part of the challenge. But work force resistance doesn’t help. “Training the C-Level is a big challenge,” noted one member. “They often present the greatest risk, but are the shortest on time and desire.”

Attendees resolved to focus on developing the “right” training, along with creative means for capturing attention and attendance.

#### **2. Create/update an accurate inventory of information assets and supporting technologies**

All attendees resolved to undertake a step-by-step analysis to identify all information assets, along with existing and desired resources, to defend them and keep them private. Once again, given resource constraints brought on by the economic recession, it is more

*See, 10 privacy resolutions, page 36*

## Did You Know?

### **Password insecurity**

Researchers found that the top five most-popular passwords of one million users of a social networking site are 1) 123456 2) 12345 3) 123456789 4) password, and 5) iloveyou, leading one CTO to comment that humans might have a genetic flaw that prevents them from choosing strong passwords.

*Source: New York Times*

### **Weaning off the Web**

The South Korean government has established Internet Rescue camps to treat individuals who have developed online addictions. Two-week intensives led by Internet addiction counselors have helped youths wean themselves off the Web. Treatment includes activities intended to recapture childhood lost to virtual environments, such as outdoor activities.

*Source: Frontline*

### **10 million addicts**

In China, an estimated 10 to 14 percent of adolescent Internet users qualify as “addicted” to the Internet. That’s about 10 million teens.

*Source: Frontline*





**IAPP members:**

**Does your organization offer free or discounted products or services to other IAPP members?**

***If so, let them know!***

**Advertise at a DISCOUNTED RATE here in our new member-to-member benefits section.**

Contact Wills Catling at  
[wills@privacyassociation.org](mailto:wills@privacyassociation.org)  
or +1.207.351.1500, ext. 118



**MEMBER to MEMBER Benefit**

**Debix Is The Only Data Breach Solution That's Proven To Work.**



Since August 2007, Debix has stopped over 1,400 identity theft attacks.

**Debix Breach Solutions Include:**

- The only electronic identity theft network
- The industry's best price
- \$25,000 of identity theft insurance
- Breach Response Specialists
- Weekly and monthly reporting.

Sign up for your free year of protection.\* Go to [www.Debix.com/iapp](http://www.Debix.com/iapp)

To learn more about Debix Breach Solutions, call 800-965-7564 or go to [www.debix.com/breach](http://www.debix.com/breach)

\*Offer limited to registered IAPP Members.



10 privacy resolutions

*continued from page 35*

important than ever to understand what's at stake.

**1. Implement and/or update the privacy risk management program**

Everyone agreed that a new year calls for a fresh look at the "risk" programs. Having obtained a good inventory of information assets and defenses, a good risk analysis is the natural next step. "A good risk-management program is particularly essential in these lean economic times," noted one participant. "Businesses need to get the biggest bang for their buck."

**Personal resolutions**

On a personal level, each participating member resolved to take care of their own identities, too. Topping the "personal" resolutions were: shredding all mail and sensitive documents before they

*"A good risk-management program is particularly essential in these lean economic times. Businesses need to get the biggest bang for their buck."*

end up in the trash; getting a lock for the home mailbox; and signing up for fraud alerts.

**Keeping resolutions**

Only time will tell whether these resolutions fall by the wayside in the face of limited resources, limited time, and com-

peting demands. But the old saying is that "if you aren't careful, you'll end up exactly where you are headed." So, if anything, setting resolutions is as much about correcting course as fully meeting each resolution.

*Luis Salazar is a shareholder in the Greenberg Traurig Miami office and a member of the firm's Business Bankruptcy and Reorganization Department and Data Privacy and Security Law Task Force. He is a member of the IAPP Publications Advisory Board. He can be reached at [salazarl@gtlaw.com](mailto:salazarl@gtlaw.com).*

*Jorge Rey is a manager at Florida-based Kaufman, Rossin & Co., one of the top accounting firms in the Southeast region in. He provides consulting services in IT Security, Information Management, and e-Discovery. He can be reached at [jrey@kaufmanrossin.com](mailto:jrey@kaufmanrossin.com).*