Privacy and electronic health records in Canada

By Michael Power

The federal and provincial governments of Canada have invested billions to develop health information technology, but privacy concerns loom. Public support for EHRs, says Michael Power, will be tied to how well patients’ private information is protected. Power describes Canada’s EHR landscape here.

In Canada, the provinces and territories manage and deliver health services to their residents; the federal government provides a large degree of funding under the authority of the Canada Health Act, which specifies criteria and conditions that provinces and territories must meet in order to qualify for financial transfers.

To facilitate the sharing of health information among healthcare providers across the continuum of care, the federal government, through Canada Health Infoway, has made significant investments in regional and provincial electronic health record systems. To date, Infoway has invested $1.6 billion and committed a further $500 million in early 2009 to several hundred EHR projects. The provinces have also contributed significant funds to implement healthcare information technology.

See, Electronic health records, page 3

“New HIPAA” poses important challenges for business associates

By Kirk Nahra, CIPP

Kirk Nahra sheds light on the primary changes to HIPAA privacy and security requirements resulting from the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act. He discusses challenges and offers compliance strategies for business associates.

The new Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements, imposed by the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), will have a significant impact on the privacy and security of healthcare information, and on the compliance obligations for affected healthcare companies. While the healthcare industry itself struggles to implement these new requirements, the biggest changes may impact HIPAA business associates—the service providers to the healthcare industry. These companies—for the first time—will be covered directly by most of the HIPAA rules. Meeting these new requirements will be a substantial challenge, and business associates need to move quickly to develop an appropriate plan to ensure compliance by the February 2010 HITECH deadline.

See, New HIPAA, page 5

This Month

- Global Privacy Dispatches ................. 12
- On notice ............................................. 20
- Privacy’s nutrition label ....................... 21
- On consent .......................................... 22
- Privacy classifieds .............................. 23
- Proposed new Consumer Financial Protection Agency ......................... 24
- IAPP Leadership opportunities ........... 28
- 2 on 201 ................................................ 30
- Pulling rank: privacy pro survey results ... 31
- CIPP graduates ................................. 31
- Privacy news ...................................... 34
- Calendar of events ............................. 38
A testament to the growing importance of data privacy is the fact the IAPP now has more than 6,200 members worldwide. It is a down economy. We are all doing more with fewer resources. Yet data privacy issues, and the professional field that deals with them, continues to expand.

The data privacy headlines reflect this growth. In the past six weeks: Germany’s Bundestag passed legislation to restrict marketers’ data collection practices; the U.S. Federal Trade Commission again extended the enforcement date for the Red Flags Rule; Iran President Mahmoud Ahmadinejad implemented a data retention law; and Morocco’s King decided to create a commission for the protection of personal data. Data breach notification laws took effect in two more U.S. states and Pakistani officials rolled out new RFID-enabled driver’s licenses.

Elsewhere, Maine legislators enacted a law restricting marketers’ collection and use of minors’ personal information; computer scientists created “self-destruct” software for digital data; and Canada’s federal privacy commissioner released the findings of an extensive, first-of-its-kind investigation into the privacy practices of a major social networking site.

The space and the issues are heating up. We are covering all of the above-mentioned topics, and many more, at the IAPP Privacy Academy. If you haven’t already, please visit www.privacyacademy.org to discover the breadth of practical knowledge up for grabs at this year’s Academy. If ever there was a good time to push for professional development resources, the time is now. Massachusetts Attorney General Martha Coakley is among nearly 80 Academy presenters. Her keynote address, and the breakout sessions to follow it, will give conference-goers the confidence and practical know-how they need to come into compliance with the strict requirements set out by MA 201 CMR 17. (More info on page 30.)

I hope to see many of you in Boston.
Electronic health records
continued from page 1

It is important to emphasize that “EHR” in Canada specifically refers to patient-centric, longitudinal health record systems that contain a subset of data of interest to multiple providers. Electronic medical records (EMRs) in Canada, on the other hand, are provider-centric and contain substantial patient detail that may not be of interest to other providers. This distinction does not appear to apply in the U.S.

Most of the development to date has focused on infrastructure and systems to digitize and transport key elements (e.g., network, applications, registers) and electronic medical record systems in hospitals. Because of a low level of EMRs held by primary care providers, adoption and implementation of EMRs (a necessary component in any EHR system) is moving to the forefront as the next challenge to address. A number of provinces are moving to an ASP model for EMRs (British Columbia, Ontario, Alberta, Nova Scotia and Saskatchewan).

Privacy and security considerations loom large because EHRs, in the Canadian eHealth model, are designed to facilitate the sharing of data for patient care, public health surveillance, and health research, and in electronic communication between and amongst patients and providers. For patients, there is a fear of undesirable consequences, including financial loss or the loss of personal dignity (e.g., discrimination or social stigma) arising from the misuse of data. Public support for EHRs can be tied to how well healthcare providers and governments keep PHI private and secure.

“This statute, among other things, creates a framework for the creation of Health Information Banks...”

“Alberta’s Privacy Commissioner has been critical of these changes and the enactment of these amendments seems to have stalled.”

A number of provinces have health-specific privacy legislation (British Columbia, Alberta, Saskatchewan, Manitoba, Ontario) and others are contending enactment of such statutes (New Brunswick, Nova Scotia, Newfoundland). Other statutes exist that affect the collection, use, and disclosure of personal health information.

British Columbia has enacted the E-Health (Personal Health Information Access and Protection of Privacy) Act. This statute, among other things, creates a framework for the creation of Health Information Banks; allows individuals to issue “disclosure directives;” and creates a Data Stewardship Committee to evaluate research requests for information. Whether this is sufficient is debatable given the emergence of the “BC Big Opt Out” campaign (www.bcoptout.ca), which promotes “opting out” of the provision of PHI to “eHealth.” Alberta has proposed amendments to its Health Information Act to effectively dispense with consent (a custodian will no longer be required to consider a patient’s wishes about the exchange of health information via Alberta Netcare) and permitting the government to require custodians to make health information available via Alberta Netcare. Alberta’s Privacy Commissioner has been critical of these changes and the enactment of these amendments seems to have stalled.

It can be argued that the Canadian experience with the deployment of EHRs has seen technology outpace policy and concerns about privacy (or

See, Electronic health records, page 4
perhaps more accurately how to deal with privacy issues) have affected the development of provincial EHRs. The whole area of de-identification policy, the misalignment of legacy IT systems and privacy policy requirements, the need for the aggressive use of audit capabilities (i.e. a strong monitoring policy), and the lack of comprehensive privacy programs at all levels of healthcare delivery all point to further attention to privacy being necessary in order to avoid a loss of patients’ trust and confidence.

Governance and data custodianship loom large as issues where sharing of sensitive data is a major system requirement. It is arguable that current legislation and rules of conduct governing the healthcare professions do not adequately address responsibilities for health IT systems’ operations. Similarly, how EHR/EMR custodians will manage and apply consent directives across multiple patient/provider identities, domains, and even jurisdictions remains a challenge.

Privacy is recognized clearly as an issue to address and, to some degree, is being addressed. Canada Health Infoway has produced privacy and security requirements in the form of a conceptual architecture and is working with provincial and territorial representatives to address privacy governance issues. Provincial privacy commissioners remain vigilant in the enforcement of health privacy statutes, and RFPs for provincial e-health initiatives show a clear attention to the privacy aspects of such initiatives. The devil, as they say, is in the details, and EHR initiatives, whether in Canada or elsewhere, will need to demonstrate alignment between political objectives of protecting privacy and workable technical and process measures that achieve those requirements while meeting the needs for a more efficient and effective healthcare system.

Michael Power is a Toronto-based legal advisor/consultant on privacy and information risk management issues, serving both public and private-sector clients. Mr. Power writes and speaks extensively on privacy and information security issues and previously served as vice president of privacy and security at eHealth Ontario. He may be reached at emp@michaelpower.ca.
HIPAA background
The HIPAA era began with the passage of the Health Insurance Portability and Accountability Act of 1996. While “HIPAA” now means many things to many people, at its foundation, the HIPAA law focused on “portability,” the idea that individuals could “take” their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions.

When Congress passed HIPAA, it also added into the mix a variety of other topics related to the healthcare industry (such as creating large funding for what has now become more than a decade-long fight against healthcare fraud). One of the policy mandates adopted in HIPAA was to move toward standardized electronic transactions for the healthcare industry. The idea was that certain “standard transactions”—like the submission of a health insurance claim and the payment of that claim—could be standardized, and thereby create efficiency savings and more effective results. (Keep this in mind as you consider the current debate about electronic health records and their potential impact on the healthcare system). With these standardized transactions came a concern about healthcare information being put into electronic form, with the resulting requirements for the creation of the HIPAA Privacy Rule and the HIPAA Security Rule.

But this background also led to one key component of these rules: the limits on the applicability of these rules to “covered entities”—the entities (such as doctors, hospitals, and health insurers) who might be participating in these standardized transactions. The law mandated the rules—but restricted their application to those covered entities only.

Accordingly, when the Department of Health and Human Services (HHS) began to develop these rules, it was faced with a significant limitation on its jurisdiction—it could apply the rules only to covered entities. HHS developed a creative solution to respond to a key fact about the healthcare system. While the covered entities are core participants in the industry, they rely on tens of thousands of vendors to provide them services, with many of these services involving patient information. Therefore, the concept of a “business associate” was born—an entity that provides services to the healthcare industry where the performance of those services involves the use or disclosure of patient information.

Because HHS had no direct jurisdiction over these “business associates,” HHS imposed an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that...
the covered entity violated the HIPAA rules. A business associate's failure to meet a contractual privacy standard would be a breach of that contract, but would not subject the business associate to government enforcement, because the business associate was not regulated under the HIPAA rules. This system has existed since the inception of the HIPAA Privacy Rule in 2003.

The primary changes
Now, in the HITECH Act, Congress has blown this HIPAA structure to bits, by imposing direct legal compliance obligations on business associates. Although this legislation does not turn business associates into covered entities, it does impose—for the first time—direct accountability on these business associates, with potential civil and criminal liability for a failure to meet these requirements.

While there are many changes to the HIPAA rules, three developments stand out from the rest:

1. More enforcement risk
It was widely anticipated that the Obama Administration would be more aggressive about HIPAA enforcement than its predecessor. Independent of this inclination, the new legislation creates substantial new opportunities for aggressive enforcement of the HIPAA rules. Over the course of the next few years, we can expect these changes to produce a fundamental shift in the overall enforcement of the HIPAA Privacy and Security Rules.

First, the provisions increase substantially the penalties that are available for violations of the rules, from the current high of $25,000 to as much as $1.5 million. Fines are mandatory in situations involving “willful neglect.”

Second, state Attorneys General (AGs) now have clear and explicit authority to enforce the provisions of the HIPAA rules. While state AGs have initiated healthcare-related privacy and security actions in the past, relying on their inherent authority to act to protect citizens of a state, this new provision essentially creates a parallel enforcement environment for HIPAA violations. On the one hand, this enforcement is limited in meaningful ways, mainly in terms of amounts that can be sought by the state AGs. On the other hand, however, this approach creates realistic risks of differing standards and inconsistent action across differing states, most likely without the procedural protections of the HIPAA Enforcement Rule.

Third, correcting what many saw as an oversight in the prior HIPAA provisions, the legislation now permits enforcement actions against individuals employed by healthcare entities. Even though the Department of Justice has creatively pursued a limited number of criminal cases against individual employees (mainly where identity theft, healthcare fraud, or some other serious criminal activity is combined with the HIPAA issue), this new provision creates a broader and more explicit opportunity for enforcement against individuals.

2. Security-breach notification
At the same time that enforcement actions are given new strength, the legislation also creates a new federal security-breach notification requirement for the healthcare industry. Most security breaches—including many events that have not historically been thought of as security breaches—now must be disclosed not only to consumers but also to HHS and, in some situations involving larger breaches, even to the media.

This provision creates a new notification standard for the healthcare industry—whether the breach has anything to do with an electronic health record or not. While clearly there are open questions about details of the legislation, this provision is broader than most relevant state notification laws because it (1) applies to breaches involving any kind of personal information held by healthcare companies (not merely the specific categories—such as Social Security numbers—that are the subject of state laws), and (2) does not include any “risk of harm” threshold. Therefore, this pro-
vision will require reporting of a wide range of security breaches, regardless of the sensitivity of the information involved or the realistic risk of any harm from the breach.

For the healthcare industry at large, this breach-notification requirement may be the single most significant provision of this legislation—and the one that is likely to affect a large number of companies most quickly and publicly. Because the notice requirement applies only to “unsecured” information, this legislation also may accelerate the movement toward encryption of a wider range of healthcare data.

3. Extension of HIPAA requirements to business associates
The other change that will generate enormous work for the healthcare industry and its business partners will be a series of provisions that essentially extend full compliance responsibility for the HIPAA Privacy and Security Rules to the business associate category—all of the companies that provide services to the healthcare industry. Today, these vendors must sign a contract with their healthcare client that extends certain HIPAA provisions by contract to the business associate category. Again, this provision seems to have nothing to do (specifically) with electronic health records. It clearly extends HIPAA coverage to all business associates, whether they deal with electronic health records or not.

For the healthcare industry, these rules also create an apparent large-scale obligation: the need to revise all existing business associate contracts to incorporate these new requirements. Healthcare companies—with full memory of the difficulties of compliance with the initial HIPAA business associate contracting requirements in 2003—should promptly begin to develop model language and an approach to overall modification of thousands of business associate contracts.

Areas of impact for business associates
Between the extension of the HIPAA rules to business associates, the new enforcement environment, and the significant concern and confusion about security breaches, the overall risks from the healthcare privacy structure are now magnified significantly for business associates. Business associates will need to review these provisions promptly, and identify where their current compliance policies are insufficient for this new environment.

What are the major areas that will deserve attention?

The HIPAA Privacy Rule
The HITECH provisions are somewhat confusing on how the Privacy Rule will be applied to business associates. It is clear that not all portions of the Rule will

See, New HIPAA, page 8

Complimentary Trial!

From data breaches to EU and Asian data protection...

BNA’s Privacy & Security Law Report tracks the latest legal developments.

Subscribers include chief privacy officers and counsel for many Fortune 500 and other multinationals.

Try the Report FREE and see what you are missing!

Keep pace with new federal, state, and international court rulings, laws, and regulations in the rapidly changing area of privacy and data security—including financial, health, international, and online privacy law—with BNA’s weekly Privacy & Security Law Report.

The Report is the most respected source for news on significant legal developments, and helps you ensure compliance with the EU Data Directive, the FTC Act, and dozens of other privacy/security-related laws and regulations.

To begin your no-risk trial:
Visit www.bna.com/trials and input Priority Code PVLR481AA.
be applied to business associates. For example, there is no obligation for business associates to prepare and distribute a privacy notice to individual patients. This makes sense, since many business associates will be unknown to the patient community.

As a general matter, HITECH indicates that business associates must, by law, follow the provisions of the business associate contract that are mandated by the Privacy Rule. For business associates—who presumably have been following these contractual provisions for the past several years—there should be no significant new obligations; but the risks from a failure to meet these obligations have grown. All business associates should take this opportunity to re-evaluate their policies and procedures for meeting these requirements.

The HIPAA Security Rule
The HIPAA Security Rule presents significantly more challenges. Today, under a business-associate contract, a business associate has only limited obligations under the Security Rule. For example, the business associate must “[i]mplement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity.” This translates—for most business associates—into an obligation to maintain reasonable and appropriate security practices. However, now that business associates must comply with the overall HIPAA Security Rule, a substantially different compliance approach will be required. In particular, while the HIPAA Security Rule is very “process-oriented,” the detailed process is quite different from what most companies go through for reasonable security. In particular, there is an extensive list of particular topic areas for review, and the requirement to develop policies and procedures to document the choices that have been made. Accordingly, moving from “reasonable and appropriate” security standards to “HIPAA compliant” security standards may require a very substantial effort for many business associates. This effort will need to begin quickly.

Breach notification
As with many of the state laws, the obligation of a “business associate” under the HITECH breach-reporting provisions is to report a breach to the covered entity—much like the current reporting structure for “security incidents” under the Security Rule. For business associates, it will be critical to implement a program to identify these breaches, investigate them promptly and report them to customers. In addition, this provision creates some challenges for the business associate contracting process. Because the notice provision will be applicable to breaches that occur 30 days after the implementing regulation is issued—which is
required to be issued within 180 days of passage of the law—this provision will take effect before most of the other provisions of the law. Business associates should anticipate pressure from customers to execute these agreements on a quicker timetable than otherwise would be required.

**The planning process**

With these new requirements and risks for business associates, how does a business associate work its way through these challenges?

**Contracting**

The biggest challenge will be to manage the business associate contracting process. This will involve both timing and substantive issues. Companies that are business associates will want to promptly identify a strategy for this process, to assess the volume of contracts affected and the substance of what these documents should say. Moreover, companies should anticipate a wide range of new demands from healthcare customers related to these rules (and perhaps other topics as well). Companies should pay close attention to the “required” elements of a business associate contract, which will change somewhat, but not too dramatically, but also should carefully consider any proposed extension of these requirements to new or greater obligations than are required by the law.

**Security planning**

Companies need to begin their security rule compliance efforts now. For some companies, this effort will mainly involve documentation—understanding the requirements of the HIPAA Security Rule and converting current security policies and procedures into HIPAA-compliant documents. For other companies, particularly those without well-developed information-security programs, the required efforts may be much more substantial. It will be critical to involve personnel beyond the information technology (IT) department in these efforts—the Security Rule requires a variety of steps beyond the usual expertise of IT departments (involving personnel policies, training, and other areas). Moreover, when HIPAA-covered entities went through the Security Rule compliance process, they found that the biggest challenge often was to “translate” security practices into meaningful policies and procedures that can be understood by the workforce and presented (if necessary) to customers and regulators.

**Breach planning and education**

In addition to an overall security process, business associates will need to develop security-breach notification plans. These will require not only a thorough process for investigating breach reports and mitigating potential damage, but also an internal education and training plan along with a communications strategy for reporting these breaches to customers and regulators.
customers. This is an area where the risks are quite high because any security breach notification situation involves a security failure of some kind. Moreover, these breach-reporting provisions may be the most complicated part of the business associate contracting process—because covered entities will be pushing for quick reporting with detailed investigative information about the breaches, along with provisions dictating financial responsibility for the results of breaches.

**Overall compliance review**

In addition, companies must conduct an overall compliance review to ensure that appropriate practices are in place. While there clearly are new requirements imposed by HITECH, business associates also must review their existing contractual obligations and practices. While many business associates have been diligent about their overall HIPAA compliance, others have taken a more “hands off” attitude based on a “low-risk” evaluation. Given the wide-ranging set of new obligations and the increased enforcement risks, this may no longer be an appropriate risk management approach.

**Segregation of activities**

Another challenge may be more subtle, but may be very important for some companies. If your company provides services only to the healthcare industry, you may not need or want to segregate your “HIPAA” component from your other activities. For other companies—where the healthcare industry is one of many industries serviced by your company—you may wish to evaluate whether there are reasonable means of separating the healthcare practices from those other areas so that the needs for HIPAA compliance do not bleed over into areas where meeting such rigorous requirements is not necessary. This may be easier to do on the privacy side than in connection with security. In fact, an inability to complete this segregation may mean that security compliance efforts are even more significant. This issue requires a careful evaluation of the HIPAA obligations in the context of your overall business activities.

**Conclusion**

For HIPAA business associates, there are broad new compliance obligations, coupled with significantly enhanced enforcement risks. While these challenges clearly are manageable, they require careful analysis and a thoughtful plan to respond to the many likely issues.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, DC. He will present “Making Sense of the New Healthcare Privacy and Security Rules” on Friday, September 18 at the Privacy Academy 2009 in Boston.
What do you know?

Personal information – about your employees, your customers or even their customers – is everywhere within your organization, and is vital to your ability to serve customers, communicate with employees and grow the business. Protecting the privacy of that data is not optional. Customer expectations, supply chain relationships and employee connectivity all increase the complexity of effective privacy protection. Our team of professionals can help you make sense of changing technologies, complex global regulations and challenging business requirements. We provide experienced, independent advice to help protect one of your most valuable assets. Because when it comes to privacy protection, it’s not what you know – it’s who you know. Give us a call.

What’s next for your business? ey.com/privacy
The extensive complaint included 24 allegations against the company, with key issues relating to Facebook’s, collection, use, and retention of users’ personal information (PI), and its retention and security practices.

The commission’s 385 paragraph findings report includes 11 sections:

- Section 1 – Date of Birth
- Section 2 – Default Privacy Settings
- Section 3 – Facebook Advertising
- Section 4 – Third-Party Applications
- Section 5 – New Uses of PI
- Section 6 – Collection of PI from Other Sources
- Section 7 – Account Deactivation and Deletion and Accounts of Deceased Users

At the time this newsletter went to press, Facebook had not yet responded to the OPC’s compliance recommendations.
EU extends privacy on social networking sites

By Jan Dhont

On June 12, 2009, the Article 29 Data Protection Working Party (WP) adopted its Opinion 5/2009 on social networking (Opinion). In the Opinion, the WP specifies data protection requirements applicable to social networking sites.

According to the WP, the EU data protection legislation applies to the activities of providers of social networking services (SNS), even if their headquarters are located outside the European Economic Area (EEA). Although debated, the WP feels that if cookies (or other applications) are placed on a Web site visitor’s computer in an EEA Member State, such visitor’s computer qualifies as automated equipment, which triggers the application of the EU and national data protection legislation of the Member State in question.

For SNS providers to avoid clashes with European regulators, they will need to take a number of measures to ensure compliance with the WP guidelines and recommendations. These are as follows:

- To reduce the risk of unlawful processing of personal data by third parties, SNS providers should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile’s content that is beyond their self-selected contacts. Restricted access profiles should not be discoverable by internal search engines (i.e. prohibition to provide for searches by parameters such as age

See, Global Privacy Dispatches, page 14
and location) and decisions by the user to extend access to his/her profile’s content may not be given implicitly.

• In relation to information uploaded by users, the WP recommends that SNS (i) provide adequate warnings about the privacy risks involved, and (ii) require users to obtain individuals’ consent to upload pictures or other personal information. To that end, tagging management tools could be introduced, e.g. by making available areas in a personal profile to indicate the presence of a user’s name in tagged images or videos waiting for consent, or by setting expiration times for tags that have not received consent from the tagged individual.

• Publication of sensitive personal information (relating to race, religion, political views, health, etc.) is subject to the explicit consent from the data subject. In some EU Member States, images are considered to constitute sensitive personal information since they may be used to distinguish between racial/ethnic origins or to deduce religious beliefs or health data. The WP does not consider images on the Internet to constitute sensitive personal information per se, unless they are clearly used to reveal sensitive information about individuals. As facial recognition technologies improve, however, publication of images on the Internet may raise increasing privacy concerns.

• SNS providers should delete accounts that have been inactive for long periods, and discard users’ personal information after they delete their accounts. Similarly, information deleted by a user when updating his/her account may not be retained.

• Some SNS providers allow their users to send invitations to third parties. The WP considers that the opt-in restrictions on the use of electronic mail for the purposes of direct marketing do not apply here, provided that the invitation sent by the user is of a personal nature. In order to avoid said restrictions, an SNS provider must comply with the following criteria:

  (i) no incentive is given to users to send invitations;

  (ii) the provider does not select the recipients of the message (i.e. the practice by some SNS providers to send invitations indiscriminately to
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.

COME to Booth #1, at the IAPP Privacy Academy 2009 to learn how Experian can protect your organization.

VISIT experian.com/databreach for more information.

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


Jan Dhont is a partner at Lorenz Brussels. He may be reached at j.dhont@lorenz-law.com.

GERMANY

By Florian Thoma

Data Protection Act amendments

The amendments to the Federal Data Protection Act (FDPA; in German: Bundesdaten-schutzgesetz - BDSG) passed parliament (the Bundestag) on July 3, and on July 10, the second chamber (the Bundesrat - Federal Council) decided not to raise objections. The act now only needs signature by the President and promulgation. It will, with limited exceptions, enter into force on September 1, 2009.

The act is largely a reaction to recent data protection breaches involving a number of high-profile German companies, in particular retailer Lidl, Deutsche Telekom, and Deutsche Bahn (German Railways).

• The principles of data avoidance and reduced/economic use of personal data is extended from data processing systems to all collection, processing, and use of personal data. Further, personal data is to be anonymized or pseudonymized unless the efforts to do so are disproportionate (sect. 3a).

See, Global Privacy Dispatches, page 16
• Market research and opinion polling companies are required to register their systems with the Data Protection Authority (DPA) and it is mandatory for such companies to appoint a data protection officer (which is a change only for small companies that, until now, were exempt) (sect. 4d para. 4, sect. 4f para. 1).

• The role of the data protection officer is supported by a new protection against dismissal during his function and for one year thereafter (unless the employer would have the right to terminate without notice for important reasons) and must have the possibility to attend seminars and the like (paid for by the employer) to keep up-to-date with data protection-related developments (sect. 4f para. 3).

• Sect. 11 para. 2 was completely changed (last-minute change) and now contains detailed requirements on specific topics to be covered by written agreements between controller and processors. This will be one of the big challenges for companies, as this change also applies to contracts made before September 1. In particular the following topics must be addressed:
  - subject and duration of the services to be provided;
  - the types of data, the type of data subjects, type of collection and processing, and use of data, to which extent, and for which purposes;
  - technical and organizational measures to protect personal data in accordance with sect. 9 of the act;
  - the correction, deletion, and blocking of data;
  - duties of the processor in accordance with the act’s sect. 4, in particular duties to control the services;
  - if the processor has the right to employ subcontractors;
  - control and audit rights of the controller and the respective cooperation and toleration duties of the processor;
  - data breaches and non-compliance with contractual duties by the processor or his staff;
  - the extent to which the controller has the governance/rights to direction vis-a-vis the processor; and
  - deletion of data and/or the return of media following termination of the processing services.

• Also, sect. 11 para. 2 now extends the surveillance duties of the controller. Language so far is rather unspecific. Now the act requires that the controller has to verify the processor’s compliance prior to the...
start of the processing, and then in appropriate intervals thereafter. Those controls need to be documented, and missing documentation is an offense and can be fined by up to 50,000 Euro.

• The “core” of the reform was very much reduced in the parliamentary debate. Legislators started with the idea to abolish completely the so-called “list privilege,” which allowed the transfer, sale, and use of list data (titles, name and address, year of birth) and replace it with a strict opt-in principle for commercial communications/advertising. However, at the end sect. 28, para. 3 it allows the use of personal data for advertising, marketing, and opinion polling purposes if (a) the data subject has consented in writing or in specific alternative forms as provided for by sect. 3a, or (b) if data lists (limited to names, addresses, titles, job functions, year of birth) are derived from public sources and used for the marketing of one’s own products or third-party products, or transferred to third parties for their advertising; in the latter two cases it must be indicated in the ad from where the data originates (sect. 28 paras 3, 3a). Further, there are a number of formal requirements regarding the right to object and the form of notice 7 consent requirements.

• The controller may not “bundle” a contract with the data subject’s consent where the data subject does not have an alternative to obtain comparable goods and services elsewhere (sect. 28 para. 3b).

• There is a full new sect. 30a on market research and opinion polling excluding the use of data for other purposes and requiring anonymization as soon as practical.

• A new sect. 32 limits the use of employees’ data (including applicant data) to what is required for the decision whether to enter into an employment relationship, to perform the employment (e.g. salaries, tax, and social security requirements, delegations, career development), and to terminate the relationship. Specifically, the use of data to pursue criminal behavior of employees requires documented evidence and the interest of the employer to pursue this must outweigh interests of the suspected employee (adequate relation between means and goals, i.e. no excessive collection and use of data on an employee for minor wrongdoing).

• Sect. 3 of the FDPA adds a new definition of “employees,” which influences the scope of new sect. 32.

• Sect. 38 para. 5 extends the rights of the DPA. They were limited to requiring additional technical and organizational measures in the past but now can require changes and amendments to systems and in case of non-
compliant processing, shut down the whole system in question.

• Sect. 42a introduces a U.S.-style security breach notification duty for the private sector where sensitive data (special types of data, data related to criminal acts and offenses, data subject to professional secrecy duties, bank account information) has been made accessible or transferred unlawfully to a third party and grave adverse effects impend on the data subjects. The notification must be given to both the DPA and the data subjects without undue delay.

• Sect. 43 adds some new offences and raises fines (from 25,000 Euro to 50,000 for “smaller” cases and from 250,000 to 300,000 for larger ones). Also, the fines can be higher, where appropriate, to outweigh any economic advantage that results from the non-compliance.

• Sect. 47 states that, for advertising and marketing, the changes will be implemented from April 1, 2012 onwards, and for market research and opinion polling from April 1, 2010 onwards, but in both cases only to the extent the data has been collected prior to Sept. 1, 2009. All data collected after Sept. 1 is already subject to the new rules.

In addition to this act, the Federal Data Protection Act will change as of April 1, 2010, due to another recent act that is meant to limit the use of scoring techniques (in particular credit scores derived from a higher number of individual values by statistical measures to express creditworthiness of a person, as well as consumer scores), and where scoring is used to increase transparency in the data used for the scores as well as ensure better data subjects’ rights.

Thoma is the chief data protection officer at Siemens AG.

See page 22 for a global review of opt-in versus opt-out requirements for digital marketing initiatives.

NETHERLANDS

By Richard van Staden ten Brink

DPA enforces information security in hospitals

On June 2, 2009 the Dutch Data Protection Authority (DPA) took enforcement action against four Dutch hospitals because they failed to improve their information security practices.

The enforcement action results from an investigation of the Dutch Health Care Inspectorate (DHCI) in 2004 and a follow-up investigation of...
the DPA and the DHCI in 2008. In the follow-up investigation, the DPA and the DHCI investigated the information security practices of 20 hospitals. The DPA and the DHCI established that most hospitals had not implemented security policies that corresponded to industry standards such as NEN 7510 and ISO 17799, and that awareness of information security amongst staff members was low. All 20 hospitals were instructed to develop and implement action plans to improve information security or face enforcement action.

The DPA has issued administrative orders to four hospitals that did not improve their information security practices sufficiently. The orders require the hospitals to perform a security risk analysis, to appoint an information security coordinator, and to make a member of their executive boards responsible for information security. The hospitals are required to implement all orders before September 1, 2009. If they fail to do so, the DPA will impose penalty sums ranging from EUR 30,000 to 210,000 per hospital.

Richard van Staden ten Brink is advocaat at De Brauw Blackstone Westbroek in Amsterdam. He may be reached at richard.vanstadentenbrink@debrauw.com.

FRANCE

By Pascale Gelly and Elisabeth Quillatre

On site investigations: the 2009 programme

The CNIL has issued its onsite investigation programme for 2009. Areas of focus in the private sector will be:

- recruitment activities (including recruitment agencies, Internet sites, and large groups);
- the sports sector (all data processing, including video surveillance, supporters lists, and blacklists);
- the marketing sector (new techniques, new targets, Web sites, businesses in the field); and
- healthcare providers (all data processing concerning patients’ rights).

It is worth reminding readers that the CNIL annual report indicates that, in 2008 only 25 percent of onsite investigations resulted from individuals’ claims. This shows the importance of the targeted areas identified in the investigation programme.

See, Global Privacy Dispatches, page 36
On notice, consent, and radical transparency

On notice

U.S. fair information practices are founded on the concept of notice and choice, but the effectiveness of this framework has come into question in professional circles, with some suggesting that in the brave new digital world where data collection opportunities are many and data use opportunities are rich, “notice” is failing when it comes to privacy. Privacy notices, they say, are written by lawyers, for lawyers, and are too often focused on reducing legal risk as opposed to educating consumers.

During a recent interview with the New York Times, FTC Bureau of Consumer Protection chief David Vladeck said that today’s disclosures are long, defensively written, and most consumers don’t read or understand them. Even seasoned attorneys find themselves in the dark. As Vladeck told the Times, he’s been practicing law for 33 years and “can’t figure out what the hell [they] mean anymore.” Vladeck said that consent “in the face of these kinds of disclosures…I’m not sure that consent really reflects a volitional, knowing act.”

Many feel the consumer protection aspect intended by notice and choice has fallen by the wayside in the digital environment.

This is not unique to privacy. The financial services field and others are finding consumers unable to penetrate policy notices with their length and legalese. The repercussions of this paradigm can be far-reaching.

That’s radical

In a March Wired magazine exposé, writer Daniel Roth suggested that the recent financial crisis resulted, in part, due to failures of notice that prevented more people from recognizing the harbingers of collapse. In the article, “Road Map for Financial Recovery: Radical Transparency Now!”, Roth suggested that twentieth-century financial disclosure mandates result in a mass of data whose volume “obscures more than it reveals; financial reporting has become so transparent as to be invisible.” Roth suggested a new approach involving “radical transparency,” where data empowers the public for the public good:

We should tap into the massive parallel processing power of people around the world by giving everyone the tools to track, analyze, and publicize financial machinations…only when we give everyone the tools to see each point of data will the picture become clear. Just as epidemiologists crunch massive data sets to predict disease outbreaks, so will investors parse the trove of publicly

IS YOUR DATA PROTECTED?

Compuware protects your company’s private data like no one else. We deliver the people, processes and technology to help the most complex IT organizations keep sensitive data private on any platform—from test to production—without losing productivity. Compuware helps you protect your business and customers from data breaches and comply with regulatory requirements. That’s why more businesses trust Compuware for their mainframe solutions than any other IT provider in the world.

www.compuware.com/dataprivacyoffers
David Weil agrees that disclosure improvements are needed. Weil is a co-director of the Transparency Policy Project at Harvard University’s Kennedy School of Government. He and fellow directors Archon Fung and Mary Graham are working on improving disclosure practices in the financial services and other industry sectors. The researchers say that in the same way the Internet has impacted notice and choice, it can bear a “new generation of transparency policies.”

Their book, Full Disclosure: The Perils and Promise of Transparency, explains what went wrong with the initial promise of transparency policies and how a new approach could result in regulations that do much more to empower those the information was meant to help.

Archon Fung and David Weil will lead the session “Radical Transparency” at the Privacy Academy 2009, where they will present a comparative analysis of transparency in other policy areas and the parallels with the privacy sector. Fung and Weil will also deliver Friday’s keynote address.
tion label at several conferences, encouraging attendees to mark them up and send them back—has been largely positive. Several A-list companies have responded with enthusiasm and hinted they might eventually want to use the label (Cranor declines to identify them). Others have praised the snapshot the
nutrition label gives of an organization’s privacy practices, but are hoping it can be amended to include information about third-party advertising or social-networking practices.

“One thing you do lose is that very detailed bit about third-party advertising. We can represent in the grid everything that comes as a part of it, but maybe not at the level of detail some people may want,” Cranor concedes. As a result, the
label is being tweaked for online use: When a user mouses over any cell in the grid, more information will appear on his screen.

As for the future, Cranor says that the nutrition label will be built into the privacyfinder.org search engine—possibly by the time you read this. More testing is currently taking place, with Cranor et al particularly focused on whether the nutrition label deals with privacy too generically and doesn’t take into account quirks from various industries (sensitive ones like healthcare and finance vs. less-sensitive ones like retail).

Cranor is also keen to address a question she was initially asked while participating in a Federal Trade Commission workshop on the topic of privacy policies a year ago. “Somebody asked me point blank, ‘If nobody reads privacy policies, why are we bothering with them?’” she recalls. “What I told them, and what I’ve told a bunch of people since then, is that our goal isn’t that everybody reads privacy policies all the time. Our goal is that when somebody has a question about privacy, that information is there for them and that they can quickly and easily access it. We hope that we’re on our way to that.”

To subscribe to Inside 1to1: Privacy, go to www.privacyassociation.org and click on “educate.”

On consent

With all of the national and regional regulatory variations on consent, marketers will do well to carefully plan their global strategies. In an article for the August issue of Inside 1to1: Privacy, Jay Cline, CIPP, explores the global landscape of opt in versus opt out.

Read it online at www.privacyassociation.org
In the Privacy Tracker this month...

If you haven’t subscribed to the Privacy Tracker, you’re missing out!

Subscribers to the IAPP Privacy Tracker publications suite receive valuable legislative-tracking information in four parts:

- Weekly e-mail updates highlighting the week’s hottest bills
- Weekly online reports of all the week’s activity on privacy-related legislation
- Monthly e-newsletters featuring bill and law analysis provided by privacy experts from DLA Piper and Hogan & Hartson
- Monthly subscriber-only calls, where privacy experts provide insider information on hot bills and answer your questions

Subscribers also get access to the Privacy Tracker Web site, which features audio conference and newsletter archives and downloadable monthly activity reports.

Stop by the Privacy Tracker information booth at the IAPP Privacy Academy 2009 or e-mail privacytracker@privacyassociation.org to request demo access to Privacy Tracker today!

---

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.

- **PRIVACY POLICY COUNSEL**
  Google
  Washington, DC

- **PROGRAM SPECIALISTS – (FREEDOM OF INFORMATION ACT)**
  U.S. Department of Homeland Security
  Washington, DC

- **INFORMATION ASSURANCE PRIVACY CONSULTANT, MID-LEVEL**
  Booz Allen Hamilton
  Washington, DC

- **INFORMATION ASSURANCE PRIVACY CONSULTANT, SR. LEVEL**
  Booz Allen Hamilton
  Falls Church, VA

- **PRIVACY OFFICER**
  U.S. Department of Homeland Security, Office of Intelligence and Analysis
  Washington, DC

- **GLOBAL PRIVACY COUNSEL**
  eBay Inc.
  San Jose, CA (possibility for EU placement)

- **PRIVACY ANALYST**
  eHealth Ontario
  Toronto, Ontario

- **SR. MANAGER, PRIVACY AND INFORMATION/CORPORATE OFFICER**
  ATB Financial
  Edmonton, AB

- **SR. ATTORNEY – PRIVACY AND DATA PROTECTION**
  Manpower
  Milwaukee, WI

- **POLICY ADVISOR – PRIVACY, TECHNOLOGY, AND ONLINE TRUST**
  TRUSTe
  Washington, DC

---

The Lighter Side of Privacy

Reprinted with permission from Slane Cartoons Limited.
Administration proposes new federal Consumer Financial Protection Agency

By Heidi C. Salow and Micah R. Thorner, DLA Piper

The Obama Administration’s proposed sweeping changes to financial services regulation include the creation of a new consumer-protection bureau—The Consumer Financial Protection Agency (CFPA). The plans have raised questions about the potential for new disclosure standards in the financial-services industry. In this article, Heidi Salow and Micah Thorner of DLA Piper provide a brief overview of the proposed CFPA and the privacy uncertainties the plans present.

Addressing the Obama Administration’s proposals to reform financial regulation in the U.S., Barney Frank (D-MA), Chairman of the House Financial Services Committee, promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourned for its August recess at the end of July.

This proposed new agency would be authorized to concentrate, in one agency, many of the consumer protection powers over mortgages and credit cards that now are spread across as many as 10 federal regulators. The Obama Administration proposal is set forth in a Department of the Treasury report, “Financial Regulatory Reform: A New Foundation” (Report).

The report reflects the Obama Administration’s view that a broad reorganization of the way the government regulates its financial system and protects consumers is necessary because consumer protection has allegedly taken a back seat to other aspects of bank regulation. This view follows the issuance, in the waning months of the Bush Administration, of strong credit card regulations by the Federal Reserve Board, compounded by the recent enactment of legislation that threatens to dramatically alter the existing business model that has historically governed the credit card industry.

“If these reforms have many legislators and businesses very worried.”

The Obama Administration’s proposed sweeping changes to financial services regulation include the creation of a new consumer-protection bureau—The Consumer Financial Protection Agency (CFPA). The plans have raised questions about the potential for new disclosure standards in the financial-services industry. In this article, Heidi Salow and Micah Thorner of DLA Piper provide a brief overview of the proposed CFPA and the privacy uncertainties the plans present.

Addressing the Obama Administration’s proposals to reform financial regulation in the U.S., Barney Frank (D-MA), Chairman of the House Financial Services Committee, promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourned for its August recess at the end of July.

This proposed new agency would be authorized to concentrate, in one agency, many of the consumer protection powers over mortgages and credit cards that now are spread across as many as 10 federal regulators. The Obama Administration proposal is set forth in a Department of the Treasury report, “Financial Regulatory Reform: A New Foundation” (Report).

The report reflects the Obama Administration’s view that a broad reorganization of the way the government regulates its financial system and protects consumers is necessary because consumer protection has allegedly taken a back seat to other aspects of bank regulation. This view follows the issuance, in the waning months of the Bush Administration, of strong credit card regulations by the Federal Reserve Board, compounded by the recent enactment of legislation that threatens to dramatically alter the existing business model that has historically governed the credit card industry.

“If these reforms have many legislators and businesses very worried.”

The Obama Administration’s proposed sweeping changes to financial services regulation include the creation of a new consumer-protection bureau—The Consumer Financial Protection Agency (CFPA). The plans have raised questions about the potential for new disclosure standards in the financial-services industry. In this article, Heidi Salow and Micah Thorner of DLA Piper provide a brief overview of the proposed CFPA and the privacy uncertainties the plans present.

Addressing the Obama Administration’s proposals to reform financial regulation in the U.S., Barney Frank (D-MA), Chairman of the House Financial Services Committee, promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourned for its August recess at the end of July.

This proposed new agency would be authorized to concentrate, in one agency, many of the consumer protection powers over mortgages and credit cards that now are spread across as many as 10 federal regulators. The Obama Administration proposal is set forth in a Department of the Treasury report, “Financial Regulatory Reform: A New Foundation” (Report).

The report reflects the Obama Administration’s view that a broad reorganization of the way the government regulates its financial system and protects consumers is necessary because consumer protection has allegedly taken a back seat to other aspects of bank regulation. This view follows the issuance, in the waning months of the Bush Administration, of strong credit card regulations by the Federal Reserve Board, compounded by the recent enactment of legislation that threatens to dramatically alter the existing business model that has historically governed the credit card industry.

“If these reforms have many legislators and businesses very worried.”

The Obama Administration’s proposed sweeping changes to financial services regulation include the creation of a new consumer-protection bureau—The Consumer Financial Protection Agency (CFPA). The plans have raised questions about the potential for new disclosure standards in the financial-services industry. In this article, Heidi Salow and Micah Thorner of DLA Piper provide a brief overview of the proposed CFPA and the privacy uncertainties the plans present.

Addressing the Obama Administration’s proposals to reform financial regulation in the U.S., Barney Frank (D-MA), Chairman of the House Financial Services Committee, promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourned for its August recess at the end of July.

This proposed new agency would be authorized to concentrate, in one agency, many of the consumer protection powers over mortgages and credit cards that now are spread across as many as 10 federal regulators. The Obama Administration proposal is set forth in a Department of the Treasury report, “Financial Regulatory Reform: A New Foundation” (Report).

The report reflects the Obama Administration’s view that a broad reorganization of the way the government regulates its financial system and protects consumers is necessary because consumer protection has allegedly taken a back seat to other aspects of bank regulation. This view follows the issuance, in the waning months of the Bush Administration, of strong credit card regulations by the Federal Reserve Board, compounded by the recent enactment of legislation that threatens to dramatically alter the existing business model that has historically governed the credit card industry.

“If these reforms have many legislators and businesses very worried.”
The CFPA would be charged with ensuring that consumers have clear information about the financial products or services they purchase, as well as protecting them from any deception they might encounter when purchasing such products. The proposed legislation suggests that the agency could accomplish these objectives by requiring lenders to make safer, “plain vanilla” products clearly available to consumers, while stepping up scrutiny on alternative products. The agency would be empowered to issue new regulations requiring financial disclosure documents to “balance communication” of the relative merits of the products or services, “prominently disclose significant risks and costs,” and communicate those risks and costs in a “clear, concise, and timely” manner. In short, the Administration proposes a reform of financial services regulations that purport to integrate the consumer perspective, by rule, into the marketing and sale of financial services and products.

These reforms have many legislators and businesses very worried. Some of their key concerns about the proposal include:

1. **Broad authority over financial products.** Under the terms of President Barack Obama’s plan, the new agency would have sweeping authority over providers of financial products, including banks and credit card companies. The authorization language in the proposal is very broad and so the precise impact of any forthcoming regulations is difficult to gauge. Nonetheless, many in the financial services industry have expressed grave concerns about whether this proposal will add yet another layer of regulation and whether the federal government, in the form of CFPA, will soon be dictating the terms of the products the industry offers—for example, the rate and fees that can be charged to credit card customers—and whether rules that are virtually unreviewable could meaningfully alter their business models and threaten their economic viability. In addition, given the broad language used to define the concepts of financial services and products in this new proposed statute, and the extensive delegation of authority provided to this new agency by the contemplated legislative provisions, it is possible that jurisdiction may be asserted over products and services not traditionally seen to be within the scope of conventional financial services and products. One consequence of being subject to such jurisdiction would include the possibility of non-recognition of an agreement to arbitrate.

See, *New CFPA proposal, page 26*
2. New regulator with less knowledge.
The proposal removes responsibility for consumer protection from the existing federal banking agencies and Federal Trade Commission and sequesters it in a new federal agency with no other defined purpose other than to “promote transparency, simplicity, fairness, accountability, and access in the market for consumer products or services.” The CFPA would be charged with protecting consumers of credit, savings, payment, and other consumer financial products and services, except for investment products and services currently regulated by the SEC. The FTC would retain authority for dealing with fraud, remain the lead agency for data security, and have backup authority for the CFPA. The new agency, however, would become responsible for privacy protection related to financial products, services, and transactions.

Because the CFPA’s supervisory, examination, and enforcement authority would extend to all persons and entities covered by the statutes it implements, as well as by statutes with no or limited rule-writing authority (such as the Fair Credit Reporting Act [FCRA] or Gramm-Leach-Bliley Act [GLBA]), all federal and state-chartered depository institutions, bank affiliates, and other nonbanking institutions would fall within its jurisdiction despite the new agency’s limited knowledge of financial regulations issued across multiple federal agencies.

In other words, critics contend, the new agency would have enforcement authority without the necessary technical and institutional expertise to successfully protect consumers. It should be added that enforcement authority for this new agency not only contemplates the ability to litigate free of the Justice Department in federal courts, but also to represent itself before the United States Supreme Court following notice to the U.S. Attorney General.

Because most, if not all, financial services products would be regulated by one agency, it is possible that such a structure would give the CFPA only some of the information it would need for effective regulation, making the whole system weak and inefficient.

3. New disclosure standard creates uncertainty for financial services companies. In March 2007, eight federal regulators (the Board of Governors of the Federal Reserve System, the Commodity Futures Trading
Commission, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller, the Office of Thrift Supervision and the Securities and Exchange Commission) requested comment on a model privacy form (Model Form) that financial institutions would be able to use for their privacy notices to consumers, as required by GLBA. The agencies made clear that use of the Model Form (expected to be finalized in August) would be entirely voluntary but would allow entities to qualify for a safe harbor. Achievement of safe harbor status would depend on vigorous adherence to the content and format requirements set forth in the proposed rule, however. The information contained in the proposed Model Form is highly standardized, permitting very little variation among entities’ disclosures about their information-sharing practices.

The Administration’s proposal would potentially limit the ability of financial service providers to obtain this safe harbor by using the Model Form. The Administration’s Report proposes that the CFPA enact regulations:

- making all mandatory disclosure forms clear, simple, and concise;
- requiring that disclosures and communications with customers be clear and reasonable; and
- allowing the CFPA to use technology to make disclosures more dynamic and relevant.

The plan would require financial service providers to present disclosures that are “technically compliant, non-deceptive, and reasonable.” To satisfy this new standard, marketing materials, notices (including privacy notices), and other consumer communications would have to identify any significant product risks, and a provider that failed to meet this duty would be subject to action by the CFPA. When introducing a new product or service, a provider would risk liability—even for using a Model Form—unless the provider obtained a “no action letter” or waiver from the CFPA.

In light of these specific proposals for consumer notices and communications, it is unclear at this early juncture whether the proposed Model Form will become obsolete.

Conclusion

Given the role that abusive and overly complex exotic mortgage products played in sparking the financial crisis, at first glance an independent agency dedicated to consumer financial protection might not seem terribly radical. But the true impact of such a new federal bureaucracy, operating with a singular purpose yet in the absence of any true institutional context, lies in the many details to be unveiled as the legislative process evolves. Already, many serious questions have arisen, with answers yet to come.
Brodden your privacy portfolio

Become an IAPP leader

*Six thousand members. Hundreds of volunteers. The privacy profession and the IAPP continue to experience rapid growth. But we need your help! Be one of the hundreds of IAPP members worldwide who are actively engaged in building the privacy profession as advisory board members with the IAPP.*

Eligible members are encouraged to apply for volunteer leadership opportunities on one of the IAPP’s advisory boards, including its board of directors. Most terms will begin in January, 2010.

Submit your nomination(s) by October 30.

**Education Advisory Board**
The Education Advisory Board supports the creation of compelling and timely programming for IAPP conferences and audio series. The boards convene for monthly conference calls, during which members offer guidance on emerging privacy trends and issues, and recommend programming on global privacy issues that beginner and advanced privacy pros need to know. Other contributions include networking with peers to promote, support, and field inquiries on IAPP event programming.

**INSIDE 1to1: Privacy Advisory Board**
In conjunction with Peppers & Rogers Group, the IAPP publishes the monthly e-newsletter, *INSIDE 1to1: Privacy*, which explores the relationship between privacy and trust. Privacy pros on this advisory board convene monthly by teleconference with Don Peppers and Martha Rogers to generate story ideas relevant to privacy and trust. Privacy thought leaders, practicing privacy pros, and attorneys are encouraged to lend their expertise on this board and help guide insightful editorial content for this popular e-newsletter.

**Privacy Advisor Advisory Board**
Help guide the coverage of privacy and security issues for the Privacy Advisor, the IAPP’s monthly newsletter. The success of this important member benefit depends upon you, our members, who make sure the content is useful and fresh. This advisory board convenes once each month by teleconference, where members suggest timely, relevant content based on their work in the field of privacy. Besides meaningful participation in the monthly conference call, members of this board are expected to provide articles for the publication. Members may also be asked to recruit potential authors.

**IAPP Certification Advisory Boards**
IAPP certification advisory boards meet regularly via teleconference to provide insight into and perspective on certification course requirements, testing protocols, continuing education, and program oversight. Opportunities exist to develop future credentialing programs. The IAPP seeks senior privacy officers, attorneys, and consultants with demonstrated subject matter expertise in the areas covered under IAPP privacy credentialing programs: foundation course (CIPP), U.S. government (CIPP/G) and Canadian privacy (CIPP/C).

**IAPP Canada KnowledgeNet Chairs**
KnowledgeNet Chairs organize meetings in their respective cities for IAPP members. The Office of the Privacy Commissioner of Canada has provided a grant to help establish KnowledgeNet chapters in cities across Canada. As a result, all meetings in 2009-2010 will be open to all individuals wishing to attend.

**IAPP Canada Advisory Board**
The IAPP Canada Advisory Board (CAB) comprises a minimum of 12 privacy professionals who actively participate in developing programming and content for IAPP Canada. A two-year commitment is required. Members will provide guidance and strategic input, and serve as leaders in the promotion of IAPP Canada and all of its programs and activities. Nominations may be submitted at any time during the year. Candidates, or those nominating on another’s behalf, should include in their nomination brief biographical data and an objective for serving on the CAB.
IAPP Board of Directors
The IAPP Board of Directors comprises a minimum of 18 privacy professionals who actively participate in various aspects of IAPP operations. A five-year commitment is required for this board, whose members work to help the organization achieve its mission. Nominations may be submitted at any time during the year. Candidates, or those nominating on another’s behalf, should include brief biographical data and an objective for serving on the board of directors in their nomination. The Nominating Committee will consider candidates late in the year, and will forward its recommendations to the full board of directors for consideration and election.

FREE PASSES CONFERRED
Many of you recently completed the IAPP member survey. Congratulations to the following members whose names were selected in the free conference pass raffle. See you at the Privacy Academy!

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

Peter Lee, CIPP
Sutter Health

Learn the latest on privacy without ever leaving your office.
Visit the IAPP’s online Educational Library.

SPECIAL IAPP AUDIO CONFERENCE PACKAGE
Get a comprehensive view of the latest issues in healthcare privacy with these two recent audio conferences. Find out what you need to know NOW about electronic health records and employee privacy!

Healthcare Privacy and the New Federal Stimulus Package: Understanding the Requirements
New Health Privacy Challenges in the Workplace

Order both for just $250 USD.

Buy it today at www.privacyassociation.org/edulibrary

IAPP ADVISORY BOARD QUALIFICATIONS
The Nominating Committee will assess nominees based on their qualifications, including, but not limited to:

- Participation in IAPP conferences
- CIPP status
- Submission of articles to IAPP publications
- Existing leadership roles within the IAPP
- Industry diversity, geographic diversity and gender/race/ethnic diversity

Please send nominations by October 30 to J. Trevor Hughes, CIPP, IAPP Executive Director at: jthughes@privacyassociation.org.
2 on 201

Two Privacy Academy sessions to focus on MA 201 CMR 17

Two sessions at the Privacy Academy will focus on a law that has brought much anxiety to privacy pros nationwide:


On Thursday, September 17, regulators, enforcers, practitioners, and industry representatives will help attendees understand the requirements in the session “Massachusetts Data Security Regulations: Perspectives From Regulators, Enforcers, Practitioners, and Industry.” Session leaders say: “If you counsel businesses that hold the personal information of others—including all businesses that accept credit card payments—this session is for you.”

Massachusetts Attorney General Martha Coakley will deliver a keynote address before the Wednesday session.

IdentityForce™
Your Trusted Partner in Identity Protection.

Only one identity protection company received Best in Class from Javelin Strategy, is the #1 provider of Data Breach services to the Federal Government, and is endorsed by the American Hospital Association.

Visit us at booth #12 to learn more or call 877-IDFORCE

www.identityforce.com
Pulling rank

In a recent survey of privacy professionals in North America and abroad, privacy leaders ranked where their position falls within their organizations, revealing that 61 percent are only one or two reporting levels from the CEO. Twenty-seven percent of respondents were within three levels from the organization’s CEO.

Here’s the full breakdown.

Levels between Privacy Leader and CEO

<table>
<thead>
<tr>
<th>Position Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>One level (direct report)</td>
<td>16</td>
</tr>
<tr>
<td>Two levels</td>
<td>45</td>
</tr>
<tr>
<td>Three levels</td>
<td>27</td>
</tr>
<tr>
<td>Four levels</td>
<td>11</td>
</tr>
<tr>
<td>Five levels</td>
<td>0</td>
</tr>
<tr>
<td>Six levels</td>
<td>2</td>
</tr>
</tbody>
</table>

All Privacy Academy attendees will receive the full findings of the Ponemon Institute-International Association of Privacy Professionals benchmarking survey at the conference.

Register online at: www.privacyacademy.org.

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 June 2009:

Genet Alemu, CIPP
Marylene Nallan Arakeri, CIPP
Abhishek Bakre, CIPP
Lori D. Baruch, CIPP
Tejinder Basi, CIPP/C
Helen Beckuchi, CIPP
Vikas Bhatia, CIPP
Saralee Cowles Boteler, CIPP
Pamela Loomar Bushnell, CIPP
Charles A. Castille, CIPP/G
Sandep Chopra, CIPP
Michael Edward Clark, CIPP
Lisa Leigh Clemmer, CIPP
Megan B. Colletti, CIPP
James Anthony Conz, CIPP
Catalin Cosovanu, CIPP
Brian D. Dan, CIPP
John Robert Deane, CIPP
Roie Edery, CIPP
Michelle R. Escobar, CIPP
Mary Ines Faria, CIPP
Molly M. Gavin, CIPP
Jacques Franck Gilbert, CIPP
Theodore Glasser, CIPP
Brian Stevenson Hall, CIPP/G
John Paul Halvorsen, CIPP
Shane Erik Hannaford, CIPP
Francine Hanson, CIPP
Mary L. Harter, CIPP/G
James Vincent Holzer, CIPP/G
Charlotte Marie James, CIPP/G
Tiekier Johnson, CIPP/G
Tiffany Olson Jones, CIPP
Sreenivas Kancharla, CIPP
Gene Edward Katzorke, CIPP
Toshiaki Robert Kawaguchi, CIPP
Robert Khatladouhairi, CIPP
Catherine S. Kirkman, CIPP
Daniel Lee Kittle, CIPP
William Joseph Krojewski, CIPP
Christina Langlois, CIPP/G
Kimya L. Lashgari, CIPP
Dickson Leung, CIPP
Cathryn Lockwood, CIPP/G
Jeremy Allan Logsdon, CIPP
Brian Loomis, CIPP
Melissa Susan Manis, CIPP/G
Arlene Martin, CIPP
Carla Mauney, CIPP/G
Bridget M. McGurk, CIPP
Jean Marie McKenzie, CIPP/G
Grace Sung Ehn Meng, CIPP
John M Mesrobian, CIPP
Judy Rinderle Miller, CIPP
Sarah Mitchell, CIPP
Karen L. Morgan, CIPP
Teresa K. Munyon, CIPP/G
Molly Newman, CIPP
Kathy Nielsen, CIPP/G
Stacie M. Notariano, CIPP
Isabella B. Noyola, CIPP
Michael John O’Rourke, CIPP/G
Betsy Paneque, CIPP
Malcolm Parker, CIPP
Jessica Joanne Rickenbach, CIPP
Theresa Michelle Rose, CIPP
Venkat Sethi, CIPP
Robert Sean Sherman, CIPP
Ellen H. Siegel, CIPP
Robin M. Singleton, CIPP
Mark Edward Steinhoff, CIPP
Ray Stibbe, CIPP
Laurie Strand, CIPP
Stephen George Sutherland, CIPP
Anna S. Tang, CIPP
Linda S Thomas, CIPP/G
Melinda Kaye Thompson, CIPP
Matt Tocek, CIPP
Matthew D. Todd, CIPP
Bethany Cantrell Tuttle, CIPP
Sunil Varkey, CIPP
Randy R. Wanis, CIPP
Cheryl White-McLeod, CIPP
Clay Dallas Young, CIPP
CALL FOR PAPERS

The IAPP will begin accepting presentation proposals for the Global Privacy Summit 2010 during the first week of September. The 2010 Global Privacy Summit will take place in Washington, DC next March.

Visit www.privacysummit.org

Did You Know?

Offshoring? Chart course here.
Canada’s Privacy Commissioner has released guidelines to help clarify how the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to cross-border data transfers. Find “Guidelines for Processing Personal Data across Borders” at www.privcom.gc.ca.

R U cybersmart?

DPI’s deep value
The global market for deep packet inspection products will reach $1 billion by 2010.
Source: Light Reading Insider

Empire statement
The New York State Consumer Protection Board is asking citizens to consider 10 questions before engaging in online activities. The “Make Privacy Your Policy” program encourages residents to take care with what they post online and to educate themselves on how their personal information might be collected, used, or shared by online companies. www.consumer.state.ny.us/internet_security.htm
THANK YOU TO THE IAPP PRIVACY ACADEMY 2009 SPONSORS
Researchers at IBM’s Haifa, Israel Lab have developed a screen-masking software to help organizations protect the privacy of sensitive information by blocking it from view on computer screens.

Dubbed MAGEN (Masking Gateway for Enterprises), the software uses optical character-recognition technology to blank out certain onscreen information before it reaches a user’s monitor. Researchers anticipate the software will be especially useful to organizations that outsource transactions involving sensitive personal information.

ibm.com/research

Swire joins Obama administration

The privacy field’s loss is the executive office’s gain. Peter Swire, CIPP, has joined the ranks of the National Economic Council, where he will work on issues related to housing, finance, and mortgages.

This is Swire’s second White House foray. He served as chief counselor for privacy in the Office of Management and Budget during the Clinton Administration. He also served on the Obama-Biden transition team last year.

You could say Peter Swire wrote the book on privacy. He authored the first IAPP Certified Information Privacy Professional textbook, among many other privacy papers and publications. Peter’s trusted voice on privacy matters and his dedication to solving the problems of the day has nurtured the privacy field to its current standing.

The IAPP wishes Peter great success in his new role.

Gray joins IMS

Kimberly Gray has joined market intelligence firm IMS as its chief privacy officer, Americas. Gray will direct all privacy-related activities for IMS operating companies in the U.S., Canada, and Latin America.

Gray is a former IAPP board member with more than a decade of experience in privacy and data protection. Prior to joining IMS, she was chief privacy officer for Pennsylvania health insurer, Highmark.

“We look forward to Kim’s leadership in upholding IMS’s 50-plus year tradition of maintaining the most rigorous privacy standards,” said IMS Americas president Bill Nelligan.

www.privacyassociation.org
Practical privacy

In June, privacy pros came together at the IAPP Practical Privacy Series in Silicon Valley to ramp up on some of privacy’s most pressing issues.

Facebook hires Allan

Facebook has appointed Richard Allan to head up its lobbying efforts in the European Union. Allan is the former head of European regulatory affairs for Cisco.

In March, the company hired former American Civil Liberties Union lawyer Timothy Sparapani as part of its Washington operations.

Facebook Chief Privacy Officer Chris Kelly told the Guardian newspaper that, as Facebook grows, it is essential that global government officials “understand our philosophy.”

Caprio joins McKenna

Daniel Caprio has joined the Government Affairs practice at McKenna Long & Aldridge LLP as Managing Director. Caprio will counsel clients in the areas of data and information privacy, RFID, and cybersecurity.

“Our clients will benefit from [Caprio’s] strategic insight and applied experience implementing privacy laws, policies, and practices at the federal level,” said Doug Farry of the firm’s Federal Government Affairs team.

Winning with privacy

The Office of the Privacy Commissioner of Canada (OPC) has awarded a Queen’s University student with $2,500 and the opportunity to be published. Mathew Johnson won the OPC’s first-ever essay competition. Johnson studies law and public administration at Queen’s. His essay, “Protecting Privacy in Public: The Need for Public Surveillance Regulation in Canada,” was chosen out of 18 submitted.

Privacy After Hours

Mark your calendars for the next Privacy After Hours event

Thursday, October 8

Held at locations worldwide, Privacy After Hours gatherings have become popular post-work networking events.

Watch the Daily Dashboard for locations and information, or go to: www.privacyassociation.org.
Global Privacy Dispatches
continued from page 19

Fifteen recommendations for enhanced privacy

Privacy in the era of digital memory. For an increased trust between citizens and the information society. This is the title of the information report made on behalf of the Legislative Committee of the Senate on May 27, 2009 and released on June 3, 2009.

In this report, the Legislative Committee of the Senate, mindful of privacy in the digital era, issues a series of 15 recommendations highlighting areas to be improved in order to better guarantee the right to privacy. The report results from an assessment of the main threats to civil liberties: video-surveillance, PNR, cookies, proliferation and interconnection of police files, social networks, RFID, highway tolls, and so on, in order to make citizens aware of the need to protect privacy and to become a free and informed “homo numericus.” Data protection is presented as a fundamental pillar of our society.

The first three recommendations aim to strengthen awareness on personal data:

• To strengthen the importance attached to awareness on issues related to privacy and personal data in school programs;

• To promote the organization and the launch of a large-scale information campaign in order to sensitize citizens on privacy challenges in the digital era as well as to inform them about their rights under the Data Protection Law;

• To promptly promote the creation of labels identifying and promoting software, applications, and systems providing enhanced guarantees for the protection of personal data. In this respect, a recent law has simplified the process for the CNIL to deliver quality labels (see July Global Privacy Dispatch).

Other recommendations aim to increase the legitimacy of the CNIL:

A tax to fund the CNIL – Supported by CNIL president, the idea is to create a “low-cost” fee, to be paid by large public and private organizations that process personal data (just like what already exists in Great Britain). We heard at the AFCDP conference (see story below) that the government is not in favour of this approach yet, but instead agreed to increase the budget of the CNIL.

Creation of decentralized antennas – To further strengthen its activities and its fields of investigation, the CNIL would ensure its presence in France through the creation of decentralized antennas. At the AFCDP conference, Alex Türk shared that this will not happen in the near future, but that the CNIL will soon open a second branch in Paris.

A mandatory DPO – For all public and private companies of more than 50 employees, a DPO shall be appointed. Among all 15 recommendations, this one, along with the security breach notification recommendation, is the most likely to impact businesses if it ever comes to life.

To make public the hearings and the decisions of the litigation committee of the CNIL – Among recommendations to complement the current legal framework, the Senate calls for a clarification of the legal status of the IP address. Considered as a personal data by the Article 29 Working Party and the CNIL, but not by some French court decisions, the debate about how to characterize IP addresses remains open. Senators have become convinced that the IP address is “a way to identify an Internet user, such as a postal address or a phone number.” Thus, the senators argue that the IP address is personal data and should be protected as such.

Moreover, the senators support the ongoing momentum towards the definition of international standards in the field of personal data protection. The senators are also in favour of the creation of a minima of an obligation to notify the CNIL of security breaches. The CNIL would then consider whether individuals should be notified as well.

Furthermore, the creation of police files should be under the sole authority of the legislator.

The senators also believe that the legislature should consider the creation of a right of “heteronymat” and a “right to oblivion.”

As for the last (but not least) recommendation, the senators wish to raise the principle of privacy as a constitutional principle. However, Alex Türk mentioned at the AFCDP conference that a revision of the constitution is unlikely to happen soon.

For most of these recommendations, it is still a bit early to tell whether they will be brought to life by the government and the legislature. One can be sure that with Alex Türk being both at the head of the CNIL and a Member of the Senate, they will be strongly supported.

The role and future of data protection officers

The AFCDP (French Association of Data Protection Correspondents) held its 5th annual conference in Paris in June. The theme was “The Future of The Profession of Data Protection Officer: Status and Perspectives.”

Present were Alex Türk, Article 29 Working Party president and CNIL president; Gérard Lommel, Türk’s counterpart in Luxemburg; and representatives of the profession from several countries, including data protection officers from Groupama and Novartis, and representatives from fellow associations, such as the German GDD. Bojana Bellamy represented the IAPP. She conquered the audience and convinced most attendants that it takes the brain of a woman to be data protection officer. IAPP Board Vice-President Nuala O’Connor Kelly sent a message to the audience and the members of AFCDP to share her enthusiasm about the IAPP-AFCDP sister relationship.

This conference presented an opportunity to take stock of DPOs in Europe and to discuss the function of the DPO and its development. In addition to France, Germany, Luxembourg, the Netherlands, and Sweden, the countries of Estonia, Hungary, and Slovakia have
Privacy protection as an investment
The ICO wants to establish a sound economic case that will help organisations provide those who make expenditure decisions with a clear rationale for investing in proactive privacy protection. With this objective in mind, the ICO has invited interested parties to bid to undertake a three-month research project aimed at developing a business case for investing in privacy.

The completed research project, “The business case for investing in proactive privacy protection,” will help organisations put a figure on not having proper data protection and privacy safeguards in place. The report produced by the successful bidder will enable organisations to: place a monetary value on information as an asset, quantify the risks of holding information, and pinpoint the financial and reputational costs should problems occur.

Companies urged to follow revised PIA guidelines
The ICO wants companies to follow rules similar to those that apply to Government departments to ensure privacy protection when developing new IT systems or changing the way they handle personal information.

The ICO launched its latest Privacy Impact Assessment (PIA) handbook, which lets organisations assess privacy risk before implementing new technologies and procedures.

PIAs became mandatory for all central government departments following the HM Revenue and Customs’ data breach in November 2007, where personal data relating to approximately 25 million people were lost.

U.S.:
By John Kropf
Europe leads effort toward international privacy standard
The Spanish Data Protection Authority on June 11 held a second meeting to discuss a proposed draft international privacy standard. The data protection authorities involved seek to complete the document for adoption at the meeting of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Madrid this November.

Of the 14 national-level authorities in attendance, most represented EU data protection authorities (Spain, Czech Republic, France, Germany, Ireland, Italy, Portugal, the Netherlands, the UK, and several regional authorities). The European Data Protection Supervisor (EDPS) participated, as did representatives from New Zealand, Switzerland, and Burkina Faso. The United States Federal Trade Commission and Department of Homeland Security were invited to participate as observers.

The group’s biggest challenge is the nature of the document. ICDPPC had called earlier for a UN convention, and the draft documents so far have been written at least in part as “hard law.” Keeping in mind the time needed to fully develop a convention and other hard law, the authorities are considering whether to revise the document into a shorter paper setting forth more general principles, to be accompanied by an explanatory memo.

The remainder of the meeting focused on a series of substantive issues:

See, Global Privacy Dispatches, page 38
Calendar of Events

**SEPTEMBER**

2  IAPP KnowledgeNet – Philadelphia, PA

3  IAPP KnowledgeNet – Chicago, IL

16-18 Privacy Academy 2009
   Boston, MA

17  Privacy Dinner
   Boston, MA

18  IAPP Certification Testing – Boston, MA
Privacy Academy 2009
   Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

23  IAPP Certification Testing – Cincinnati, OH
   Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

30  IAPP Certification Testing – Los Angeles, CA
   Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

**OCTOBER**

7  IAPP Certification Testing – Atlanta, GA
   Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

8  Privacy After Hours

14  IAPP ANZ Annual conference
   Melbourne, Australia

14  IAPP Certification Testing – Denver, CO
   Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

15  IAPP Certification Testing –
    Washington, DC
    Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

16  IAPP Certification Testing –
    Vancouver, BC
    Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

19  IAPP Certification Testing –
    Folsom, CA
    Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

22  IAPP Certification Testing –
    Ottawa, ON
    Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

**NOVEMBER**

1  Deadline to provide feedback on PCI DSS
   www.pcisecuritystandards.org

2  Privacy by Design: The Definitive Workshop
   Madrid, Spain
   co-hosted by Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada and Yoram Hacohen, Head of the Israeli Law, Information and Technology Authority
   www.privacybydesign.ca/madrid09.htm

3  IAPP Data Protection and Privacy Workshop
   Madrid, Spain
   (Preceding the 31st annual International Conference of Data Protection and Privacy Commissioners, November 4-6)
   www.privacyassociation.org

**DECEMBER**

8  Practical Privacy Series:
    Government
    Washington, DC

To list your privacy event in The Privacy Advisor, email Tracey Bentley at tracey@privacyassociation.org.

Global Privacy Dispatches

continued from page 37

1) Definitions: This included analysis of the challenges associated with reconciling the EU concepts of controller and processor with non-EU concepts.

2) Scope of application: particularly important here was discussion of whether the standards should apply to the public sector and law enforcement, and the different issues raised in this area.

3) Sensitive data: The participants questioned whether types of sensitive data should be listed or whether the focus should be on areas where there is a risk of harm. Some reference was made to the APEC harm principle.

4) International data transfers: The participants’ assessments of the adequacy requirement were surprisingly negative. Participants suggested that other approaches should be considered, such as accountability.

5) The group discussed the nature of supervisory authorities with emphasis on the meaning of “independence.” Varying degrees of flexibility for different traditions existed.

6) Accountability principle: The discussion about focusing on accountability, a feature of the APEC privacy framework, was overall relatively positive.

7) Applicable law: Several authorities emphasized the difficulties in addressing this subject.

A new draft of the proposal is expected to be presented at the conference in November.

John Kropf is the deputy chief privacy officer and senior adviser for the U.S. Department of Homeland Security. The views expressed here are his own and not those of the U.S. Government.
Inspired Learning

The IAPP Privacy Academy 2009
September 16 - 18
Boston Marriott Copley Place

REGISTER NOW
www.privacyacademy.org
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 or +1.207.351.1500, ext. 118

Are your employees ignoring your privacy and data protection policies?

SAI Global helps you understand the requirements that shape your business and communicate those requirements to employees in ways that are both effective and memorable. With offices in 25 countries, well over a thousand clients and millions of satisfied users, we’ll help you build and sustain a privacy and data protection program that supports your governance, risk and compliance needs.

- Fully translated library of awareness and training
- Offline training alternatives
- Online searchable databases
- Measurement and reporting
- Legislative alerts

Visit our booth to learn more or phone or write for more information.

Toll free 877-470-SAIG
info.americas@saiglobal.com

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

To learn more about Debix Breach Solutions, call 800-965-7564 or go to www.debix.com/breach

*Offer limited to registered IAPP Members.