The Memorandum of Montevideo

Protecting the personal data and privacy of children and adolescents in the social networking environment

By Lina Ornelas

The Memorandum on the Protection of Personal Data and Privacy in Internet Social Networks, Specifically in Relation to Children and Adolescents—better known as the Memorandum of Montevideo—was presented in Mexico on December 3, 2009. The aim is to launch this initiative to the Latin American region and to begin a process of socialization and mobilization towards the protection of minors on the Internet. The Federal Institute of Access to Public Information (IFAI) collaborated on the writing of the memorandum and promoted the launch of the document in Mexico as the guarantee institution for data protection.

The document’s launch seeks precise, binding commitments from all the actors involved in the protection of children. It also seeks to promote the development and implementation of public policies to protect children and teenagers from the risks they encounter on the Internet, to bring about a culture of personal data protection, and to implement actions towards safe Internet use as a fundamental variable in the construction of a full digital citizenship.

See, Montevideo memorandum, page 3

The human factor in compliance: best practices from the trenches

This article is the first in a series contributed by MediaPro, Inc., in which privacy and data protection thought leaders from leading organizations share best practices for addressing the human factor in compliance and data protection programs and implementing a successful privacy and data security awareness and training initiative.

How important is the human factor in data security and privacy? More than 88 percent of data breaches studied involve human error or negligence, according to this year’s Ponemon Institute Annual Cost of a Data Breach study. Ironically, organizations invest heavily in IT tools to protect data but invest very little on training and awareness for their employees.

“And that’s a problem,” says Richard Purcell, CEO of Corporate Privacy Group. “Information privacy is assured primarily by the way people act on the job. Not so much by technologies and by other more tangible factors, but rather by the behaviors of the individuals. It’s the employee who leaves the company laptop in his car—not the overseas computer hacker—who’s a greater threat to most organizations. Most of the privacy challenges we observe have been caused by people at the very edges of the organization—staff-level employees,” says Purcell. “It is those people who

See, The human factor, page 5
Earlier this month there was a flare up in the debate about whether people care about privacy. Those on both sides of the issue presented their views at events and in the popular press.

On one side of the debate, a technology columnist offered the argument that privacy norms have changed, and that “Internet users have grown accustomed to information exhibitionism.” Things that might have once bothered a more privacy-sensitive public no longer rattle us, he said.

Days later, outgoing FTC commissioner Pamela Jones Harbour said, “Privacy is a fundamental right that people care about.”

So who’s right?

It’s a question that confounds many and, for better or for worse, the answer may be that everyone is right. Privacy can be an inherently personal set of expectations. Those expectations are certainly molded by our cultural, legal, and political environments. Yet, when we approach the issue, we do so as unique individuals with differing concerns and sensitivities. So if my privacy is not the same as your privacy, how can anyone ever have the “right” answer?

Elements of this debate played out at the FTC’s third and final roundtable this month, where representatives from industry, advocacy, academia and other groups explored the minutiae of data privacy. No one knows what the outcome of these roundtables will be. What we do know is that the debate will continue. We also know that, even if the norms haven’t changed to the degree some have stated, they are being tested. As noted by panelists at the IAPP’s tenth anniversary celebration this month, in the coming months and years privacy professionals will need to decipher the new privacy norms and community values and figure out how to accommodate them.

This work undoubtedly will shape our conversations in the months ahead. If you missed our tenth anniversary telecast, I urge you to watch the video on our Web site.

We look forward to seeing many of you at the Global Privacy Summit in Washington, DC next month.

J. Trevor Hughes, CIPP
Executive Director, IAPP
An international collaboration
The Memorandum of Montevideo was written at the international seminar, Rights, Adolescents, and Social Networks on the Internet, held in Montevideo, Uruguay last July for the purpose of protecting children in the information and knowledge society sphere. At the invitation of IIJusticia and the International Development Research Centre (IDRC and CRDI), several individuals collaborated on writing the document. Subject-matter experts, members of parliament, academics, data protection authorities, and global non-governmental organizations all participated, in addition to the assistant privacy commissioner of Canada and with the sponsorship of the Canadian government.

Taking a holistic approach toward the protection of personal data is an essential idea of the memorandum, which provides a series of recommendations to the actors directly involved in the protection of personal data and children. The recommendations are divided by topics and actors, such as educational authorities and agencies, parliament, the state system, justice authorities, the industry, and social civil society in general.

Balancing benefits and risks
Although the Memorandum of Montevideo recognizes that the Internet and digital social networks have become invaluable tools for accessing and exchanging information, it also recognizes that both have led to the extreme phenomena, with a particular focus on the Internet and digital social networks.

It is important to mention that, to date, Mexico has 27.6 million Internet users, 52 percent of whom are children and youngsters between the ages of 12 and 19. A considerable percentage, it is easy to understand that the memorandum’s recommendations were very much welcome. Distinguished members of the both chambers, the industry, and the state, as well as federal education authorities and social civil society representatives, participated in the event, which had a positive impact on media coverage.

Building a data protective culture
It was an extremely productive encounter. Punctual commitments were reached towards the protection of children while building the culture of personal data protection in Mexico. Members of the industry—particularly Microsoft and Google—were willingly open to add up efforts in the educational and preventive aspects, contributing in the expansion of programs to create a safer Internet and to promote safe and discrimination, sexual exploitation, and pornography on the other. Undoubtedly, the risks that children could encounter on the Internet can affect their well-being and future development.

The specific gender and cultural diversity features of Latin America and the Caribbean were taken into account prior to issuing the recommendations, as were the variety of policies and regulations concerning approaches towards the information and knowledge society phenomena.

“A specific gender and cultural diversity features of Latin America and the Caribbean were taken into account prior to issuing the recommendations…”

“Punctual commitments were reached towards the protection of children while building the culture of personal data protection in Mexico.”

See, Montevideo memorandum, page 4
The members of the upper and lower chambers of Mexico’s bicameral legislature underlined the importance of having a specific federal regulation on the subject of data protection towards fully complying with child protection and international standards. Although Mexico has recognized the right to data protection as a fundamental and autonomous right, it has not issued a specific law in the matter. Participants reached several conclusions at the discussion, mainly that data protection—that of children and adolescents included—requires an adequate institutional design in which the IFAI could be the guarantee institution of data protection—as it is already in charge of protecting data in the public archives of the federal executive branch.

Civil society representatives from several NGOs emphasized the use of the Internet as highly personal space with benefits and risks. Despite the benefits of online social networks as new social spaces, the networks are not risk-free spaces, especially for children. The evolution of technology has generated a new socialization paradigm because the use of the Internet is no longer passive, but has moved towards a more active role. Therefore, there is a social responsibility to protect and promote a full digital citizenship.

Digital citizenship education
The conclusive arguments underlined the need for actors—particularly those in charge of education—involved in taking responsibility and action, so that safe Internet use is included in the educational agenda, as well as in school-based prevention programs, embedding digital-citizenship education.

Finally, the launch of the Memorandum of Montevideo represents a regional initiative aimed at promoting a data protection culture, encouraging public policies, and incorporating the issue into the national and regional agendas.

For more information on the Memorandum of Montevideo, go to: http://memorandumdemontevideo.ifai.org.mx/.

Lina Ornelas is general director of classified information and personal data at the Federal Institute of Access to Public Information in Mexico and a co-writer of the Memorandum of Montevideo.
The human factor
continued from page 1

actually have a very strong ability to cause a significant data breach.”

Michael Jernigan, the compliance training manager for Microsoft’s Office of Legal Compliance, agrees, stating, “We’ve got somewhere in the neighborhood of 100,000 full-time employees and probably that many contingent staff. And it only takes one employee to do something really foolish to significantly impact the entire company legally and financially. The fact that the ‘foolish’ act is most likely unintentional, and/or due to being uninformed, emphasizes the need for training at all levels of the company.”

Like Microsoft, The Procter and Gamble Company sees data security as a foundation for a solid global privacy program. With buy-in from the highest levels of management, the company has implemented a comprehensive, enterprise-wide training program to address the human factor in data protection. Sandra Hughes, CIPP, the executive in charge of global ethics, compliance, and privacy at P&G, says, “For us, the human factor is everything. We can have the best systems and processes and standards in the world, but unless people are following them, it isn’t going to mean anything.”

Hughes continues, “You’re always going to have those mistakes that happen inadvertently—and that’s where your systems and processes have to come in. When employees are thoroughly trained in solid data protection practices, you’re able to quickly fix those unintentional breaches, adjust or create new processes, and then communicate this new knowledge with effective training so that it doesn’t happen again.”

Robert Posch, senior director of global compliance training for the Schering-Plough Corporation, believes that companies must “influence the individual colleague at the company so they understand not just that PII (personally identifiable information) is important, but how it applies to what they do and how they do their job, so that they buy into the value of doing it right.” Individual employees have to understand that security and privacy breaches can not only impact the company as a whole but also their own career success and job security, according to Posch. “They have to see a long-term payoff” for data security compliance, he says.

Larry Ponemon, the Ponemon Institute’s chairman and founder, says, “Ultimately, people are the ones who use and manage the data, so leaving basic elements such as training and education out of the equation is foolish.” And yet the Ponemon Institute’s study revealed that only 57 percent of respondents were addressing data protection with employee training and education.

So why do so many organizations have lax—or non-existent—data privacy and security training? “I don’t think people really understand the huge risk that they’re taking,” Jernigan says. Although some data breaches have led to expensive class action settlements, the Ponemon Institute reports the most negative and significant cost impact results from lost confidence and trust in the company, which translates directly into customer turnover—and in the case of a severe breach, potential loss of brand equity.

Jernigan believes that is why it’s incumbent on company management and executives “to really understand the risk and do whatever needs to be done in order to mitigate those kinds of potential occurrences.”

Getting buy-in from the organization’s executive team is a critical step, says Zoe Strickland, vice president and chief privacy officer for Wal-Mart Stores, Inc. “Once the company executives decide they want a privacy program that includes training and awareness, they’ve made a commitment and expect to see results. But too many times they simply don’t know how to get it done.” Strickland credits executive teams that recognize the bottom-line value of training, but admits, “They don’t know what that means to the people who have to implement it. What’s the best channel to give training and to whom? What are the key messages? You’ve got a lot of work to do to help them understand the process for employee education and the ongoing support they will need to provide.”

John Block, MediaPro’s director of compliance curriculum, agrees with Strickland’s assessment. “The challenge for most privacy and security professionals is that training and awareness are not normally on their resume. So when they’re asked to plan, create, and implement a company-wide data protection program, they have no idea where to start. As a compliance officer, you may know everything about data privacy and

See, The human factor, page 6
security regulations, but nothing about best practices in adult education that will really lead to a positive change in employee behavior."

While MediaPro works with many Fortune 1000 companies, Block is still surprised by the number of companies that forego formal training in favor of a halfhearted or cobbled-together internal program, or even no training at all. "Training may be the most visible and important item of communication an employee receives to understand your message. You really need to get it right. The quality of the message reflects on you and the organization. If it’s a half-hearted approach, employees may not take the message seriously."

He continues, "There is a widespread perception on the part of privacy and security professionals that if training is engaging and effective, then it must be beyond their budget. The reality is that high-quality online training is quite affordable, especially when compared to the cost of data breach recovery."

Block says that "By applying even a few time-tested training best practices, organizations can reap the benefits of a focused and successful implementation strategy. The ultimate goal is to provide training and awareness that enables an informed workforce to reduce security and privacy risks and forge strong customer relationships."

Richard Purcell agrees. "Ultimately, you have to educate employees on good DP practices and to understand the consequences of misbehavior. It becomes a lot easier to get things done at that point."

MediaPro would like to thank Richard Purcell, Michael Jernigan, Sandra Hughes, Robert Posch, Larry Ponemon, and Zoe Strickland for their contributions to this article. John Block has worked in the training industry for close to 30 years and directs the development of compliance courses at MediaPro, Inc. He can be reached at johnb@mediapro.com.
Healthcare privacy in 2010

By Kirk J. Nahra, CIPP

A lot is happening in the healthcare world, with the implications of healthcare reform leading the list. What can we expect to see as the major developments in healthcare privacy and security in 2010?

The HITECH era begins

At the top of the list is the commencement of the Health Information Technology for Economic and Clinical Health (HITECH) Act era, in February 2010, with implementation of most of the new changes required by the act. The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) is still promising additional regulatory guidance to help explain some of the more confusing or ambiguous provisions of the law. For many companies, such guidance may be too little, too late, especially for the companies that were hoping the OCR would provide guidance on the new requirements for business associate contracts.

So, covered entities are moving, some more quickly than others, to revise their overall Health Insurance Portability and Accountability Act (HIPAA) compliance plans to meet these new requirements. At the same time, the business-associate community now must comply with not only many of the core provisions of the HIPAA Privacy Rule, but also the very challenging overall requirements of the HIPAA Security Rule. Many business associates seem to remain unaware of these requirements, particularly those for whom healthcare clients represent only a modest proportion of their overall business. Will these “partial” business associates (for example, an accounting firm whose services to healthcare clients amount to 10 percent of its overall business) be held to the same standards as a company whose sole or primary function is to provide services to the healthcare industry (such as a pharmacy benefits manager or third-party administrator)? In any event, we can expect to see a flurry of business-associate contracting over the next few months, along with significant activity by business associates as they realize the full extent of their new HIPAA/HITECH obligations. Business associates of all stripes need to be aware of this new reality—all are subject to the full range of HIPAA laws, and will need to expand their compliance efforts accordingly, and quickly.

Will we see significant new enforcement?

The other primary effect of the February implementation is the full impact of the new enforcement provisions of the HITECH Act. While (as HHS made clear in its interim final regulation) the new penalty provisions are in effect for current violations of the existing rules, February brings new opportunities for broader enforcement, both in terms of the new HITECH provisions and the new breach regulations, and affecting the entire business associate community (which had not previously faced any enforcement risks). Additionally, state attorneys general across the country now have the ability to enforce their own versions of the HIPAA rules. Will we actually see more enforcement? And will HHS continue its overall approach of reasonableness, or will it move more aggressively to bring significant enforcement actions against those who violate these rules?

While the healthcare industry certainly should anticipate more enforcement of the HIPAA rules (if only because there has essentially been none to date), a seismic shift in the

See, Healthcare Privacy in 2010, page 8
March • 2010

Healthcare privacy
continued from page 7

overall enforcement approach is not likely. While there certainly have been situations (both in this author’s experience and in various public reports) wherein HHS enforcement appeared unfair or inconsistent with the HIPAA provisions, HHS has, in almost all situations, been reasonable in how it has investigated and concluded its enforcement activities. It has appeared to recognize that the HIPAA rules contain confusing elements, which will certainly be exacerbated by some of the HITECH provisions. Moreover, HHS has appeared to understand the difference between unintentional or innocent violations and egregious efforts to bypass HIPAA requirements.

Clearly, there will be ongoing efforts to pursue individuals and their employers where healthcare information is used inappropriately (e.g., healthcare fraud, identity theft, sale of information to others). There may even be increased enforcement in situations involving no obvious harm, but where a violation clearly occurred (such as the “snooping only” prosecution that was initiated recently). Nonetheless, while we can expect more enforcement, companies still will benefit from conscientious efforts to meet the requirements of the HIPAA and HITECH rules, as HHS has demonstrated a significant willingness to factor a company’s compliance efforts into the overall resolution of its enforcement initiatives. We can expect this policy to continue even though HHS now has significantly more enforcement tools available to it.

How will breach reporting change?

Closely related to the question of overall enforcement is how the healthcare industry will deal with the new security breach notification regulation. This regulation—which went into effect in September 2009—alters dramatically the landscape for reporting of security breaches. While the HHS regulation clarified that the HITECH Act incorporated a notification threshold of a “significant risk of harm” to individuals whose information is subject to a breach, many questions remain open about how security breaches will be reported. In addition, while HHS provided an interim period wherein there would be no penalties issued for violations of this regulation, that period ended in February, coinciding with the arrival of compliance duties concerning the remaining portions of the HITECH Act. In addition, because the HHS regulation itself is an interim regulation, HHS has, essentially, provided the healthcare industry with a five-month opportunity to prove its bona fides in connection with breach reporting. If HHS is not satisfied with the results, it has the opportunity to revise the regulation. The healthcare industry needs to be aware of the tenuous nature of this interim regulation, and must undertake to responsibly report breaches where there is a legitimate reason for reporting.

Accordingly, the healthcare industry needs to focus substantial attention on issues related to security breaches—both in terms of how best to prevent them in the first place, and also on the investigation, assessment, and notification obligations that will result when a breach does occur. Issues related to security breaches have become the single biggest focus of attention in the healthcare privacy and security debate; breaches are where public attention is centered, where the media and regulators pay the most attention, and where enforcement efforts have been concentrated. Now, with the individual notice

“The healthcare industry needs to be aware of the tenuous nature of this interim regulation, and must undertake to responsibly report breaches where there is legitimate reason for reporting”

risk and various “public confession” elements of notification imposed by the rule, breaches will receive even more prominence in the public debate. Therefore, it is critical that covered entities and their business associates take significant steps to enhance their overall security for protected health information and take careful and conscientious steps to evaluate breaches and provide notification in appropriate situations. We can expect to see lots of discussion and debate about these issues over the next few months, and to see initial steps by HHS to respond to public (and nonpublic) reports of breaches.

How will the “Meaningful Use” principles affect privacy and security?

With all of the focus on the privacy and security implications of the HITECH Act and the impending effective date for these new requirements, many in the healthcare industry have almost forgotten that the driving force behind these HITECH changes was the new incentives provided to doctors and hospitals to implement electronic health records systems. (This may be because these incentives apply to only small portions of the healthcare industry, and because the privacy and security changes essentially have nothing to do with these incentives, despite the links asserted by Congress—will Congress and HHS recognize that there may be other significant types of healthcare providers who also should be receiving “incentives” to move towards electronic health records?) But there are also important impending steps in the movement towards electronic health records, starting with the issuance of the “meaningful use” regulations by HHS, setting forth both the conditions for obtaining the financial incentives and the new standards that will be required across the healthcare industry for electronic health records in the future. These standards likely will generate extensive debate; moreover, they may be the first step in ascertaining whether we will be able to achieve the three-pronged goals of implementation of electronic health records for the purposes of cost sav-
ings, enhanced patient safety, and improved healthcare quality.

“De-identification” and research issues
On a broader policy level, we also will see developments in the ongoing debate about some of the potential public benefits of healthcare information. On the one hand, there is significant ongoing discussion about whether there is a need to re-evaluate the HIPAA standards for “de-identification” of personal health information. This information is used widely for many purposes; some (such as research) are generally lauded and others (for example, those in connection with various marketing activities) receive more criticism. (This debate has even extended to the “privacy” interests of doctors in connection with their own prescribing habits, as several state laws and perhaps even federal legislation will restrict or prevent the use of prescriber data for marketing purposes by pharmaceutical companies, even where no identifiable patient data is used.) The question is whether technological improvements and numerous additional sources of data make this idea of “de-identification” less viable, because it may, in fact, be too easy to “re-identify” information in certain situations.

At the same time, there also is a substantial debate about the public benefits of research for the healthcare community, and whether the current privacy rules create undue impediments to effective research. The possibilities presented by electronic health records and various forms of health information exchanges exacerbate these issues. These exchanges may maintain substantial volumes of incredibly useful data for research purposes; will the rules for these exchanges allow these benefits to be achieved? We will be watching both of these issues in 2010, with an eye toward both practical and regulatory/legislative efforts.

The HHS studies
Beyond the HITECH requirements, Congress also wrestled with making a far more extensive set of changes to the overall HIPAA environment. In rejecting various proposals that had been incorporated into some of the preceding legislation, Congress ultimately directed HHS and the Government Accountability Office to “study” many of these controversial issues. These studies will begin to be released in 2010. We will be watching to see if these studies lead to new potential legislation, or whether the concerns raised in earlier versions of the HITECH Act have been reduced or eliminated by other developments. Specifically, in the HITECH legislation, HHS was directed to issue a variety of studies or guidance that will play a role in the next generation of privacy regulations or legislation. These include studies or guidance related to:

• what constitutes ‘minimum necessary’ under HIPAA;

• privacy and security requirements for entities that are not covered entities or business associates, including requirements relating to security, privacy, and notification in the case of a breach of security or that should be applied to: (i) vendors of personal health records; (ii) entities that offer products or services through the Web site of a vendor of personal health records; (iii) entities that are not covered entities and that offer products or services through the Web sites of covered entities that offer individuals’ personal health records; (iv) entities that are not covered entities and that access information in a personal health record or send information to a personal health record; and (v) third-party service providers used by a vendor or other entity described above to assist in providing personal health record products or services;

• the definition of “psychotherapy notes” with regard to including test data that is related to direct responses or other materials that are part of a mental health evaluation;

• recommendations for a methodology under which an individual who is harmed by an act that constitutes an offense may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense;

• the best practices related to the disclosure among healthcare providers of protected health information of an individual for purposes of treatment of such individual; and

• guidance on how best to implement the requirements for the de-identification of protected health information.

Conclusion
So, in 2010, the healthcare industry will face a substantial set of challenges—new privacy and security rules, for both the industry and its vendors, a significant new notification provision relating to security breaches, and the expectation of significant new enforcement of these rules. At the same time, the industry will be dealing with the fallout from healthcare reform and a set of new studies and guidance that may lead to a second wave of new changes. It should be an interesting year for privacy and security in the healthcare industry.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, DC, and is the editor of the Privacy Advisor. He can be reached at 202.719.7335 or knahra@wileyrein.com.
Corporations that operate in and collect or process personal data in Asia-Pacific countries need to have comprehensive privacy policies addressing these countries’ data privacy laws. Is it possible to create a single policy that achieves such a broad coverage? The answer is yes, but Asia, unlike Europe, does not have broad regional directive requiring member states to enact local data privacy laws conforming to certain principles. Instead, Asia has only the APEC Privacy Framework (2005) that provides voluntary guidance that may inform the passage of local statutes. Therefore, corporations must consider the specifics of each country’s statutes and how these protect local information. Fortunately, Asia privacy laws to date are more similar than dissimilar in the principles they follow. This article will first review the principles of the APEC Privacy Framework and then compare the Asian countries’ privacy laws to those APEC principles. From this, a model set of corporate privacy principles will then be suggested, to provide a single privacy framework that corporations can implement and use for all of the countries throughout the Asia-Pacific region where they do business.

**APEC Privacy Framework**

Asia-Pacific Economic Cooperation (APEC) is a forum for facilitating economic growth, trade, cooperation and investment in the Asia-Pacific region. Its member countries are Australia, Brunei Darussalam, Canada, Chile, People’s Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei (Taiwan), Thailand, the U.S. and Vietnam. APEC members have endorsed a framework for the use of personal data based on a single set of principles. The framework encourages “the development of appropriate information privacy protections ensuring the free flow of information in the Asia-Pacific region.” It is generally consistent with the Organisation for Economic Cooperation and Development’s (OECD) 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability).

The nine APEC-endorsed Privacy Principles are as follows:

- **Preventing Harm** (P1): To individuals from the wrongful collection and misuse of their personal information.
- **Notice** (P2): The controllers of personal information should provide clear statements about their practices and policies, before or at time of collection.
- **Collection Limitation** (P3): Information should be lawfully collected and only if relevant to the purpose of collection.
- **Use of Personal Information** (P4): The only exceptions to the use of the information being different than the purpose of collection is if consent is given by the individual or to provide a product or service the individual requested, or if required by law.
- **Choice** (P5): The individual should be given a choice on the collection, use and disclosure of their personal information.
- **Integrity of Personal Information** (P6): Data should be accurate, complete and up to date.
- **Security Safeguards** (P7): Controls should prevent unauthorized data access, loss, use, modification or disclosure and be proportional to these risks and information sensitivity.
- **Access and Correction** (P8): Individuals should be able to access and correct their personal information, unless the burden of doing so is disproportionate to the risk for legal or corporate compliance reasons or to not compromise another individual’s privacy.
- **Accountability** (P9): The information controller is accountable and must ensure personal information transferred to a third party is protected in accordance with these principles.

**Asia-Pacific Country Privacy Laws**

The table on page 12 maps the privacy laws of the Asia-Pacific countries against the APEC Framework and each other. The numbers refer to the local privacy statute’s designated principles (P) or articles (A) that may be similar to but not necessarily the same as the privacy principles in the APEC Framework. The similarities may exist only at a high level, as each country’s privacy law has its own unique and often subtle detail-level differences.

See, Asia-Pacific data privacy, page 12
THE IAPP GLOBAL PRIVACY SUMMIT 2010

CHOOSE FROM More Than 70 Sessions and Hear From More Than 130 Speakers—the Most Programming Ever Offered!

FEATURING Special Keynotes From:

Dan ARIELY
Behavioral economist and author of *Predictably Irrational: The Hidden Forces That Shape Our Decisions*

Scott CHARNEY
Corporate Vice President, Trustworthy Computing Microsoft Corporation

Viktor MAYER-SCHÖNBERGER
Author of *Delete: The Virtue of Forgetting in the Digital Age*

Register Now

www.privacysummit.org

APRIL 19-21, 2010 | WASHINGTON, DC
Washington Marriott Wardman Park
Asia-Pacific data privacy  
continued from page 10

level, as each country’s privacy law has its own unique and often subtle detail-level differences.

Of the member states that have privacy laws, the five most developed at this time are in New Zealand, Japan, Australia, Hong Kong SAR and Singapore (although Singapore’s is based on voluntary compliance). South Korea and Taiwan also have well-developed privacy laws, but are limited in application to specific industries or government. Macao SAR has the most recently implemented statute and perhaps the most comprehensive. Many Asian countries find privacy as a constitutional right and then have laws addressing narrower legal aspects. For example, India, Indonesia and Vietnam have privacy provisions in their e-commerce laws (India is not a member of APEC but clearly a major Asian country). Mongolia has had the Law on Personal Secrecy (Privacy Law) since 1995. Other countries in Asia such as Malaysia, the Philippines, and Thailand are expected to enact new privacy legislation soon, but all have been working towards privacy protection for some time. Thailand has had a privacy law since 1997 that applies only to the government, while the Philippines has had model privacy provisions for corporations, and Malaysia’s current legislation is based on a draft from 2001. (As of the submission of this article, Malaysia had just tabled the Personal Data Protection Bill. This bill contains seven privacy principles: general (consent, collection, usage), notice and choice, disclosure, security, retention, data integrity and access.)

Mainland China has no single statute for data privacy, but it does have a number of constitutional protections for personal dignity and privacy of correspondence and civil statutes covering privacy of personality and reputation. It also has privacy regulations related to the management of computer information networks, criminal privacy sanctions and provincial consumer protection regulations. A comprehensive data protection law has been in development for the last several years, most recently based on an “experts” version, which included the principles of lawfulness, protection of rights, balancing of interests, information quality, information security, and duties. This may or may not be the basis for any ultimate legislation in China.

New Zealand

New Zealand was the first country in the region to have a full privacy statute, the Privacy Act of 1993. Revisions are currently being considered to protect cross-border movement of data and align its rules with the EU’s data protection regimen. The 12 current principles are:

**Purpose of Collection of Information** (P1): Must be for a lawful purpose related to the function of the information collector (called an “agency”) and be necessary.

**Source of Personal Information** (P2): Information should be collected directly from the individual, unless the individual consents, will not be prejudiced, will not be identified or if already publicly avail-

---

### Privacy Law Comparisons

<table>
<thead>
<tr>
<th>APEC Framework</th>
<th>New Zealand</th>
<th>Japan</th>
<th>Australia</th>
<th>Hong Kong</th>
<th>Singapore</th>
<th>S. Korea</th>
<th>Taiwan</th>
<th>Macao SAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventing Harm</td>
<td>P1, P1</td>
<td>A18, A24</td>
<td>P1, P5</td>
<td>P1, P5</td>
<td>P2, P8</td>
<td>A22</td>
<td>A19 – A21</td>
<td>A10</td>
</tr>
<tr>
<td>Notice</td>
<td>P1, P4</td>
<td>A17</td>
<td>P1</td>
<td>P1</td>
<td>P4</td>
<td>A23</td>
<td>A6, A18</td>
<td>A5, A6</td>
</tr>
<tr>
<td>Collection Limitation</td>
<td>P10</td>
<td>A15, A16</td>
<td>P2</td>
<td>P3</td>
<td>P5</td>
<td>A24</td>
<td>A18, A23</td>
<td>A5, A6</td>
</tr>
<tr>
<td>Personal Info Usage</td>
<td>P11</td>
<td>A27</td>
<td>P3</td>
<td>A22, A30</td>
<td>A12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Choice</td>
<td>P8</td>
<td>A19</td>
<td>P3</td>
<td>P2</td>
<td>P6</td>
<td>A13</td>
<td>A5</td>
<td></td>
</tr>
<tr>
<td>Information integrity</td>
<td>P5</td>
<td>A20, A21</td>
<td>P4</td>
<td>P4</td>
<td>P7</td>
<td>A28</td>
<td>A17</td>
<td>A15, A16</td>
</tr>
<tr>
<td>Access &amp; Correction</td>
<td>A22, A23</td>
<td>P9</td>
<td>P1</td>
<td>A25, A27</td>
<td>A24</td>
<td>A19, A20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability (3P transfers)</td>
<td>A10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Retention</td>
<td>P9</td>
<td>P2</td>
<td>P5</td>
<td>A13</td>
<td>A5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>P10</td>
<td>A23</td>
<td>A7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>P2</td>
<td>P1</td>
<td>P6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disposal</td>
<td>P4</td>
<td>A29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unique IDs</td>
<td>P12</td>
<td>P7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country Specific</td>
<td>Secrecy (A18)</td>
<td>Combination (A9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
able or for legal or other governmental reasons.

Collection of Information from Subject (P3): The information collector should provide the individual certain information, including purpose, recipients, access and correction before collecting, unless any of the exemptions from Principle 2 apply.

Manner of Collection of Personal Information (P4): Must not be unlawful, unfair, or unreasonably intrusive to the individual's personal affairs.

Storage and Security of Personal Information (P5): Security safeguards must be in place to prevent against loss or unauthorized access, use or modification.

Access to Personal Information (P6): An individual must be able to access his/her personal information.

Correction of Personal Information (P7): An individual may request, and the agency may on its own initiative or upon request, correct information or, if it will not correct the information, attach a statement to the information of correction sought.

Accuracy of Personal Information (P8): The agency should ensure the information is accurate, up to date, and complete before use.

Information Not Kept Longer than Necessary (P9): The agency is not to retain personal information longer than needed for the purpose for which it was collected.

Limits on the Use of Personal Information (P10): To the purpose for which it was collected, unless the individual consents, will be not prejudiced, will not be identified or for legal or other governmental reasons.

Limits on Disclosure of Personal Information (P11): To those for the purpose for which it was collected or to the individual, unless the individual consents, will be not prejudiced, will not be identified or for legal or other governmental reasons.

Unique Identifiers (P12): Agencies must ensure that they do not assign identifiers unless necessary and only for an individual with a clearly established identification.

Japan
The Japanese Act on the Protection of Personal Information of 2003 protects the rights and interests of individuals and their personal data held by businesses. The basic rules are set forth in the following articles:

Specification of the Purpose of Utilization (A15): The business handling personal information has to specify the purpose and scope of use.

Restriction by the Purpose of Utilization (A16): The business cannot go beyond the scope of the purpose of utilization without the consent of the individual, except if necessary for personal safety, public health or children's welfare, or when pursuant to law.

Proper Acquisition (A17): The business must obtain personal information by lawful and non-deceptive means.

Notice of the Purpose of Utilization at the Time of Acquisition (A18): The business must notify the individual when the information is acquired or its purpose changed, except when it is clear from the circumstances or for the safety or other rights of the individual, a third party or the business, or if compromising compliance with the law.

Maintenance of the Accuracy of Data (A19): The personal data (personal information in a database) must be kept accurate and up to date.

Security Control Measures (A20): The business has to implement proper security controls to prevent loss, leakage or destruction of the personal data.

Supervision of Employees (A21): The business has to exercise appropriate supervision over its employees who handle personal data.

Supervision of Delegates (A22): The business has to exercise appropriate supervision over its third-party delegates who handle personal data.

Restriction of Provision to a Third Party (A23): Personal data cannot be provided to third parties, except if the individual consents or for the individual's safety, children's welfare, public health or compliance with laws, or when the individual can opt-out. Outsourcing personal data that achieves the purpose (e.g. payroll outsourcing) is not to a third party.

Announcement of Retained Personal Data (A24): The business must notify the individual of certain information, including the purpose of utilization.

Disclosure (A25): The business must disclose a person's data if requested by the individual, unless it may affect the personal safety or rights of the individual, third parties or the business, or violate any laws. The individual must be notified of any refusal.

Correction (A26): The individual may request changes to his/her personal data to correct it, and the business must make such changes.

Discontinuance of the Utilization (A27): When an individual requests termination of use of improperly collected or transferred data, the business must do so unless burdensome.

Explanations of Reasons (A28): The business has to explain its refusal to not honor requests by an individual concerning his/her personal data.

See, Asia-Pacific data privacy, page 14
Asia-Pacific data privacy
continued from page 13

Australia

The Federal Privacy Act of 1988 (as revised and applied to private businesses in 2001) specifies 10 National Privacy Principles (NPPs) that apply to most businesses and healthcare providers. The states and territories also have privacy laws. The NPPs are:

Collection (P1): Information must be collected only from the individual (or from a third party if individual is notified), must be necessary to the organization’s functions, done in a lawful and fair manner and must give notice to the individual.

Use and Disclosure (P2): Personal information must not be used for a secondary purpose unless the individual consents; it is not sensitive and for direct marketing within specific limitations (e.g. opt out); if health statistical information; to prevent threats to personal or public health or safety, or when pursuant to law.

Data Quality (P3): The organization must ensure that data collected is accurate, complete, and up-to-date.

Data Security (P4): The organization must use reasonable steps to avoid loss or unauthorized access, modification or disclosure of data and to destroy or de-indentify personal information that it is no longer using.

Openness (P5): The organization must openly state how it manages, collects, uses, and discloses personal information, what type and for what purpose it has the information.

Access and Correction (P6): The organization must provide an individual access to the information, except if negatively impacting health, safety, the execution of laws or litigation. It must take reasonable steps to make information more accurate when requested to do so and provide the reasons for not doing so.

Identifiers (P7): The organization must not use the identifier of another agency or disclose such information.

Anonymity (P8): Individuals can choose to not identify themselves when entering transactions with an organization.

Transborder Data Flows (P9): Personal information can be sent to a foreign country only if the recipient follows similar privacy principles, if consent is obtained or for performance of a contract that individual is party to or is in their interest.

Sensitive Data Collection (P10): Sensitive information must not be collected, unless consent is given, is required by law or for a legal claim or the person has serious health issues and cannot consent by themselves, or for certain statistical research.

Hong Kong

The Personal Data (Privacy) Ordinance of 1995 sets out six Data Protection Principles, plus limits on automated reporting, direct marketing and external data transfers (not yet started).

Purpose and Manner of Collection of Personal Data (P1): Data should be collected in a lawful purpose and manner, directly related to the purpose of collection, and notice of specified information should be given to the individual.

Accuracy and Duration of Retention of Personal Data (P2): Steps should be taken to ensure data is accurate and not kept any longer than necessary.

Use of Personal Data (P3): Data must be used for purposes directly related to collection, unless consent is obtained from the individual.

Security of Personal Data (P4): Steps must prevent unauthorized access, use or loss.

Information to be Generally Available (P5): Data user has to make available information about his/her policies and procedures, the information held and main purposes thereof.

Access to Personal Data (P6): Individual has a right to access and correct his/her data.

As of August 2009, Hong Kong sought comment on an additional 12 proposed principles. Many of these deal with penalties or enforcement, but the following are more substantive.

Sensitive Personal Data (Proposal 1): Limits on the handling of sensitive personal data.

Regulation of Data Processors and Subcontractors (Proposal 2): Either through statute or contract, data processors/subcontractors must follow the same rules as initial data users.

Data Breach Notification (Proposal 3): Individuals must be notified on loss or leakage of their personal data. This is initially intended to be voluntary.

Singapore

The Model Data Protection Code for the Private Sector is a voluntary privacy framework which has ten model principles:

Accountability (P1): Any data transferred to a third party for processing must adhere to these principles and the organization must implement appropriate policies and procedures to maintain accountability.

Specifying Purposes (P2): The purpose for which the data is collected must be documented and communicated to the individual before collection.

Consent (P3): Collection, use and disclosure of personal data requires the advanced, voluntary consent of the individual, except in cases such as where it is not possible and clearly benefits the individual, where the personal or public health or safety is impacted or when required or allowed by law. Consent may be withdrawn at any time.
Limiting Collection (P4): Collection is limited to data collected by fair and legal means needed for the purpose of processing, except if consent or for health or safety.

Limiting Use, Disclosure and Retention (P6): Without consent or other stated exceptions, data must not be used or disclosed to a third party for other purposes and will only be retained as long as necessary to fulfill the purpose under which it was collected.

Accuracy (P6): Personal data should be accurate, complete and up to date and collected directly from the individual.

Safeguards (P7): Appropriate controls must protect personal data from unauthorized access, modification, disclosure or loss, including during authorized destruction of data.

Openness (P8): Organizations should disclose their policies and procedures about managing personal data.

Access and Correction (P9): An individual should have the ability to access his personal data and request corrections thereof and organizations must notify the individual if they refuse to make such corrections and state the reasons why, if not a valid exception.

Challenging Compliance (P10): Organization must have people and processes for dealing with complaints and investigate all complaints.

South Korea
The Act on Promotion of Information and Communication Network Utilization and Information Protection of 2001 protects the personal information of consumers held by certain industries. The number of industries subject to this law is in the process of being greatly expanded by the government. The key privacy articles in the local law are:

Collection of Personal Information (A22): User consent in advance is required to gather personal information, and the collector must provide certain details to the user.

Restrictions on Gathering Personal Information (A23): Only information related to the proposed services should be collected, not sensitive data.

Utilization and Provision of Personal Information (A24): Personal information should not be used without consent unless it is de-indentified.

Entrusting of Personal Information Processing (A25): If the processing is delegated, the information provider must so notify the user and still remain liable for any work done.

Notice on Business Transfer (A26): Users must be notified if personal data is obtained in a business transfer and the new corporation becomes responsible for the data.

Designation of Persons in Charge of Administering Personal Information (A27): This person is responsible for protecting user data and handling complaints.

Protective Measures for Personal Information (A28): The provider must take the requisite technical and administrative steps to protect the personal information.

Disposal of Personal Information (A29): Service providers can destroy the data after they have completed the purpose for which it was gathered.

Rights of Users (A30): The user may withdraw his/her consent at any time and the provider must then appropriately destroy the personal information. The use may also request that his/her personal information be corrected, and the provider must do so.

Taiwan
The Computer-Processed Personal Data Protection Law of 1995 protects the processing of personal data in certain kinds of industries. The key privacy articles in this law are:

Collection and Use of Personal Data (A6/A18): Collection and use must be in good faith and not in excess of the scope necessary, and for a particular purpose and based on consent, contract or in the public domain or for research not impacting the individual.

Permit Review of Personal Data (A12): By the individual unless an exception applies.

Accuracy and Timely Amendments (A13): Personal data must be accurately maintained and be corrected if the user requests and should be deleted when purpose is complete.

Response to Requests (A15): Must occur within a fixed time limit.

Maintenance of Safety (A17): Staff must be appointed to prevent personal data from being stolen, altered, destroyed, or disclosed.

Registration / Notice (A19-A21): Companies must be registered to collect and process personal data and provide certain information about it, such as the purpose, scope, retention period, collection methods and safety plans, and publish this in newspapers.

Scope (A23): Use beyond the specific purpose is allowed only with the individual’s consent, for personal or public health or safety or injury to the rights of third parties.

International Data Transfers (A24): May be restricted if the receiving country does not adequately protect the personal data.

Macao
The Personal Data Protection Act of 2005 protects the processing of personal data. The significant privacy articles, many unique to Asia (as they are based on Portuguese law), are:

See, Asia-Pacific data privacy, page 16
Asia-Pacific data privacy
continued from page 15

Data Quality (A5): Personal data must be collected for a specific, legitimate purpose; kept accurate; processed lawfully and in good faith, and retained no longer than necessary

Making Data Processing Legitimate
(A6): Personal data may be processed only with consent or if for contractual, legal compliance or public interest reasons.

Processing Sensitive Data (A7): Is prohibited, unless consent is obtained, it is required by law or for legal claims of individual, for medical treatment or in public interest,

Combination of Personal Data (A9): Requires approval from statute or a public authority.

Individual’s Rights: The individual has the following rights:

To Information (A10): About the data controller, the purpose of the processing, rights of access and other information.

Of Access (A11): To know which information is being processed, notification of any information that requires rectification and then blocking or rectification thereof.

To Object (A12): At any time to use of a person’s data about him/her, including for use in direct marketing and for use by third parties.

Not to be subject to Automated Individual Decisions (A13): The individual can choose not to be subject if the decision was based solely on the automated processing of data evaluating personal aspects of him/her, unless allowed by law or contract.

Security of Processing (A15): The controller must take appropriate measures to ensure the personal data against unlawful access or loss, including transmission over networks. This also applies to any third party who is performing the processing for the controller.

Special Security Measures (A16): Controllers of sensitive data must ensure physical security and control media access, personal data input, use and access and data transmission, and separate personal and sensitive data and encrypt transmissions.

Professional Secrecy (A18): Controllers are bound by secrecy, even after functions end.

Transfer of Data outside Macao (A19-A20): Must be only to jurisdictions with appropriate levels of protection, unless consent is given or for performance of a contract, in the public interest or the vital interests of the individual.

Model Corporate Principles to Comply with Asia-Pacific Data Privacy Laws
To create a single corporate privacy policy that addresses all of the current privacy laws in Asia, the following 20 privacy principles must be included. In addition, proposed local Asian law revisions and selected provisions in use elsewhere (e.g. the EU and U.S.) have been included to anticipate the need for such provisions and create a comprehensive list

Conclusion
The number of privacy laws in Asia is large and getting larger, with a number of new statutes or revisions expected in 2010. As this article has shown, the differences between the current Asian privacy laws are far fewer than the similarities, as most countries adopt the same key core principles, with the biggest differences in covered entities and enforcement of the statutes. That is not to say that new or revised domestic laws in the region will follow the same rules, but trade with Europe and the Americas and their existing privacy regimes may provide a guide to the limits of any future changes. Additionally, the results from the APEC Privacy Subgroup’s Pathfinder projects may provide additional guidance on new principles. In any case, this is a very dynamic area of the law, and corporate privacy officers and counsel will need to frequently revisit their privacy policies to ensure that their corporations stay in compliance with the changing privacy rules in all the Asian countries where they do business.

Thomas J. Shaw, Esq., is an attorney, CPA, CIPP, CISM, ERMP, CFF, CISA, CITP, and CGEIT based in Tokyo, Japan. He works with corporations across Asia to develop their legal, e-discovery, information security, data privacy, compliance, and information governance policies and procedures to assess, prepare for, and respond to litigation and technology risk. He can be reached at Thomas@tshawlaw.com or on the Web at www.tshawlaw.com.

Privacy Principles

Limits on Collection
Limits on Use and Disclosure
Right of Access and Correc tion
Notice to Data Subject
Data Security Controls/Encryption
Data Integrity
Limits on Retention Periods
Data Subject Consent / Source of Data
Limits on Sensitive Data / Security
Destruction / De-identification of Unused Personal and Sensitive Data

Data Breach Notification
Professional Secrecy
Choice / Right to Object
Supervision of Third-party Processors
Limits on Cross-border Transfers
Limits on Direct Marketing / Opt-out
Business Transfer Notification
Use of Unique Identifiers
Combination of Personal Data
Compliance with the EU Safe Harbor Rules (and other non-Asia rules)
Changes to the European Union E-Privacy Directive

By Jarno Vanto

The European Parliament approved the long-awaited amendments to the Directive on Privacy and Electronic Communications (e-Privacy Directive) in November 2009. The amendments, which are causing a stir in the world of online advertising, will be implemented in the 27 EU Member States by mid-2011.

The amendments include:

• notice and consent before cookies are placed on devices, with limited exceptions

• data breach notification obligation for communications providers and Internet service providers

• direct marketing e-mail content requirements

• the right to sue spammers, and

• strengthened enforcement powers for Member State authorities

Cookies only upon notice and consent
The general rule under the amended Article 5 (3) of the e-Privacy Directive is that the use of cookies or other software or devices enabling the storing or accessing of information already stored on the user’s terminal equipment, such as a computer or a smartphone, is only allowed on condition that the concerned user has given his or her consent, having been provided with clear and comprehensive information in accordance with the Data Protection Directive 96/46/EC, for example, about the purposes of the processing and the identity of the entity placing the cookie in the terminal equipment.

As an exception to the general rule, technical storage or access would be lawful without notice and consent for the sole purpose of carrying out the transmission of a communication over an electronic communications network, such as establishing an Internet connection, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service, such as directing a user’s shopping cart to the checkout in an online store. The placing of third-party cookies, such as those of third-party advertisers and Web traffic analysis tools, would nearly always require notice and consent because these are neither stored for the purpose of carrying out the transmission of a communication, nor strictly necessary to provide a service.

Whether this means the end of online advertising as we know it in the EU will depend upon how the requirements of clear and comprehensive notice and consent are implemented into Member State law. In this respect, the amended recital 66 of the e-Privacy Directive discussing cookies states that “the methods of providing information and offering the right to refuse should be as user-friendly as possible” and that the “user’s consent to processing may be expressed by using the appropriate settings of a browser or other application.”

In its opinion on the amendments to the e-Privacy Directive, the Article 29 Working Party, the advisory body consisting of the Member State data protection authorities, strongly objected to the use of browser settings as means of giving consent, stating that “most browsers use default settings that do not allow the users to be informed about any tentative storage or access to their terminal equipment...default browser settings cannot be a means to collect free, specific, and informed consent as required in Article 2 (h) of the Data Protection Directive.” Consequently, once the Member States have implemented the directive, their data protection authorities may take a stricter approach to consent in line with the Article 29 Working Party opinion if the implementing laws are worded in a manner that leaves room for a stricter interpretation. However, following the adoption of the amendments, Austria, Belgium, Estonia, Finland, Germany, Ireland, Latvia, Malta, Poland, Romania, Slovakia, Spain, and the United Kingdom issued a statement according to which “amended Article 5(3) is not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes,” stressing that the methods of providing information and offering the right to refuse should be as user-friendly as possible. It remains to be seen whether the commission will agree with this statement, for if there was no intent to alter the existing requirement, why was the e-Privacy Directive amended in the first place?

Transfers of cookie data outside the EU
According to Article 29 Working Party, “persistent cookies containing a unique user ID are personal data and therefore subject to applicable data protection legislation.” Thus, session cookies aside, the general requirements of the Data Protection Directive, such as fair and lawful processing, notice and consent, and restrictions on transfers of personal data outside the EU, apply to cookie data alongside the specific requirements set out in the e-Privacy Directive.

Processing of cookie data in violation of the e-Privacy Directive, without notice and consent, would clearly violate the fair and lawful processing requirement of the Data Protection Directive, making the processing illegal not only under the

See, European Union E-Privacy, page 18
European Union E-Privacy

continued from page 17

amended e-Privacy Directive, but also under the generally applicable Member State data protection laws, and would therefore also make transfers of such data outside the EU illegal.

Data breach notification

Following a lengthy debate where, for example, the Article 29 Working Party and the European Data Protection Supervisor argued for a broader scope of application for a data breach notification obligation, the amended e-Privacy Directive imposes a data breach notification requirement on telecommunications providers and ISPs.

The amended Article 2 c) h) of the e-Privacy Directive defines a “personal data breach” as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a publicly available electronic communications service in the community.” Some EU Member State legislatures, such as those of France and Germany, are in the process of introducing or have already introduced data breach notification obligations with a scope that is broader than that adopted in the e-Privacy Directive, thereby making EU-wide breach notification compliance complex and opening a door for broadening the scope of the e-Privacy Directive’s notification obligation in the future.

Pursuant to the amended Article 4 (3) of the e-Privacy Directive, communications service providers must notify data breaches to a “competent national authority,” such as a Member State data protection authority, to be defined in the implementing Member State legislation. With respect to notifying individuals, communications service providers have to make a judgment call. If the data breach is “likely to adversely affect the personal data or privacy of a subscriber or individual,” the providers must also notify the subscriber or individual of the breach without “undue delay,” unless the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures which are applied to the data affected by the breach and render them unintelligible.

According to the European Data Protection Supervisor, examples of circumstances where individual notification is required would include those where the loss could result in identity theft, fraud, humiliation or damage to reputation. Even if a provider does not notify the affected individuals or subscribers, the competent national authority may force it to do so.

The breach notification must, at a minimum, describe the nature of the personal data breach and the contact points where more information can be obtained, and must recommend measures that the recipients of such a notification can take to mitigate the possible adverse effects of the personal data breach. The competent national authorities may adopt guidelines and instructions concerning the circumstances under which providers are required to notify, the format of such notification, and the manner in which the notification is to be made. Member State authorities will also have the right to audit whether providers have complied with the breach notification obligation, and can impose sanctions in the event of non-compliance with the obligation.

(Editor’s note: For more on the breach notification requirements, turn to page 22.)

Expanded e-mail marketing content requirements

By incorporating a reference to the so-called E-Commerce Directive, the amended e-Privacy Directive clarifies the content requirements for direct marketing e-mail communications. All e-mails (including SMS and MMS) sent for the purposes of direct marketing must fulfill the following conditions:

• They must be clearly identifiable as commercial communications.

• They cannot disguise or conceal the identity of the sender on whose behalf the communication is made.

• They must clearly identify the natural or legal person on whose behalf the commercial communication is made.

• They must clearly identify promotional offers, such as discounts, premiums, and gifts as such, and make the eligibility conditions easily accessible, clear, and unambiguous.

• They must clearly identify promotional competitions or games and the conditions for participation must be easily accessible and must be presented clearly and unambiguously.

• They must have a valid address to which the recipient may send a request that such communications cease.

• They cannot encourage recipients to visit Web sites that contravene these requirements.

The sending of direct marketing e-mail communications that do not meet these requirements is prohibited.

The right to sue for spam

Pursuant to the new Article 13 (6) of the e-Privacy Directive, any natural or legal person that is “adversely affected” by violations of the Member State laws implementing the amended electronic direct marketing requirements will be entitled to bring legal proceedings for such violations if the person has “a legiti-
imate interest in the cessation or prohibition of such infringements. Thus, in addition to recipients of spam, for example corporations whose e-mail traffic is affected by spam as well as ISPs and telecommunications providers, would be able to sue the spammers in a Member State court.

Increased Member State authority powers
In addition to the existing powers of the national data protection and communications authorities, the amended e-Privacy Directive gives them the power to order an immediate cessation of the infringements of the Member State laws that implement the directive. Such cessation powers will exist alongside more traditional administrative and criminal fines and penalties. Moreover, the amendments also call for Member States to ensure that the competent national authorities have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to the amended e-Privacy Directive. Finally, the Member State authorities can adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to the amended e-Privacy Directive and to create harmonized conditions for the provision of services involving cross-border data flows.

Practice pointers
Entities whose activities fall within the ambit of the e-Privacy Directive are well advised to keep an eye on how the EU Member States implement the amendments, and should enlist knowledgeable local counsel to assist in this process. Particular attention should be paid, for example, on the following issues:

- How must notice and consent be obtained for storing cookies on devices?
- What are the specifics of the data breach notification requirement and will the Member State(s) broaden the scope of the notification requirement to cover entities other than communications service providers?
- How will the direct marketing e-mail content requirements change?
- How will the Member State(s) structure the right to sue for spam?
- What will the specific details of the Member State authority powers be and which authorities will exercise these powers?

Jarno J. Vanto is an attorney-at-law at Vanto Law PLLC in New York City. He can be reached at jarno.vanto@vantolaw.com.

NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION

REALLY? AN ORGANIZATION DEDICATED TO PROPER INFORMATION DESTRUCTION?

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

Since 1994, the National Association for Information Destruction (NAID) has been the leading proponent of standards development and education related to proper information disposal and increase employee compliance. NAID’s 1,000-plus service providers around the world are dedicated to helping organizations make informed decisions on records destruction, vendor selection, employee training, and contract language and policy development.

Get serious about information disposal - www.naidonline.org
Two recent decisions issued by a French Tribunal of First Instance (Caen Tribunal of First Instance, Interim Decision, 5 November 2009) and by the French Supreme Court (Cour de Cassation, 8 December 2009) have brought whistleblowing and the implementation of ethics helplines in French companies to the forefront of the nation’s conversation on data protection.

The evolution of perception of whistleblowing in France

In France, any processing of personal data has to be either declared to or authorized by the French data protection authority, the Commission Nationale de l’Informatique et des Libertés (CNIL). In most instances, a mere declaration of the processing is sufficient, but in cases where processing involves sensitive data or can result in data subjects being deprived of a right, contract, or benefit, French data protection legislation requires that the data controller obtain a prior authorization from the CNIL.

In consideration of the potential sanctions resulting from alleged misconducts reported by employees, whistleblowing systems, therefore, fall into the category of personal data processes subject to prior authorization.

This matter only came into discussion in France in 2005, when the CNIL denied the authorization requests for the launch of ethical helplines submitted by two French subsidiaries of U.S.-listed groups (McDonald’s France and Compagnie Européenne d’Accumulateurs, a subsidiary of Exide Technologies). The entities had submitted the requests in order to ensure their groups’ compliance with the provisions of section 301 (4) of the 2002 Sarbanes-Oxley Act (SOX).

The French data protection authority, however, considered that the systems allowed for the anonymous reporting of a large variety of alleged breaches, either to law or to internal codes of conduct which could lead to an “organized system of denunciation.”

This position raised concerns for French subsidiaries of U.S.-listed groups, which were impeded from complying with the SOX obligations. Aware of this difficulty, in November 2005 the CNIL issued guidelines aimed at clarifying both its perception of whistleblowing systems and the conditions under which such systems could be authorized.

According to these guidelines, use of the systems:

- should not be mandatory for employees
- should only be an alternative to other alert systems
- should have a limited scope

Also, use of the systems requires:

- that users and subjects of an alert be provided with comprehensive information
- assurance that appropriate security, confidentiality, and precaution will be exercised when handling alerts, and
- assurance that the system does not incite users to make anonymous denunciations

In addition to these guidelines, in December 2005 the CNIL issued a decision whereby it authorized the implementation of all whistleblowing systems matching the terms of this decision (the Standard Authorization).

French legislation authorizes the CNIL to adopt standard authorizations of this nature, simplifying the obligations of data controllers, which are then only required to register mere undertakings of compliance with the terms of the standard authorization in question. Systems not fitting strictly within the provisions of a standard authorization (e.g. broader scope of data processed, different purpose, etc.) have to be submitted to a specific authorization application.

Difficulty interpreting the standard authorization

As mentioned above, the Standard Authorization strictly defines the purposes of authorized whistleblowing systems. These must only relate to the creation of internal control procedures in the fields of finance, accounting, banking, and corruption, as imposed by French law, and the reporting of alleged violations in the fields of accounting and audit as imposed by SOX.

However, two sentences of article 3 of the Standard Authorization seem to widen this scope by providing that the “facts collected must only relate to the fields covered by the system. Unrelated facts may however be disclosed to individuals of the organisation when the vital interests of that organisation or the...
moral or physical integrity of the employees are at stake.”

This perception of a widened scope of the Standard Authorization was adopted by Dassault Systèmes and followed by the Versailles Court of Appeal in a decision of April 2008.

In this case, the works council of Dassault Systèmes initiated action further to the adoption of a new internal code of conduct, which included the implementation of a whistleblowing system that was argued not to match the scope of the Standard Authorization, and thus to be illegal.

The court dismissed these allegations. Relying on the provisions of article 3, it considered that Dassault Systèmes was entitled to expand the scope of the system for situations where “the vital interests of the group as well the physical and moral integrity of the employees were at stake.” (The helpline allowed the reporting of intellectual property rights violations, divagation of strictly confidential information, conflicts of interest, insider dealing, and sexual or moral harassment.)

However, this analysis was challenged by an interim order issued by the President of the Caen Tribunal of First Instance in November 2009. In December 2009, it was completely invalidated by the French Supreme Court.

In the first case, the works council of French company Benoist-Girard, a subsidiary of American group Stryker, requested the Caen Tribunal to suspend the company’s whistleblowing system, which consisted of an Internet Web site accessible at the address www.ethics-point.com, and which had been declared to the CNIL as compliant with the Standard Authorization.

In this framework (set out in article 3), the French Supreme Court made the same analysis on 8 December 2009 when it put an end to the Dassault Systèmes case and settled the question of the combination of articles 1 and 3 of the Standard Authorization.

The court first considered it necessary to distinguish between the purposes of the whistleblowing system (covered by article 1) and the categories of data that can be processed lawfully in this framework (set out in article 3).

According to the Supreme Court, the reach of article 3 was exclusively limited to the nature of information susceptible to being collected during an alert and could not be interpreted as extending the scope of the purposes authorized under the Standard Authorization. Article 3 was not intended at modifying article 1,” the court said.

This decision, therefore, clearly restricts the scope of the whistleblowing systems benefiting from Standard Authorization to those covering finance, accounting, banking, and corruption. This raises two final comments.

First, the position reached by the French Supreme Court can, in our opinion, be contested, as it seems to rely more on the physical location of the problematic provisions in the Standard Authorization than on the actual terms used.

Indeed, even though the terms of article 3 exclusively refer to the facts and data collected within the whistleblowing system, we perceive them as de facto extending the scope of article 1. If this was not the case, the collection of data relating to the actions endangering vital interests of the company or the physical or moral integrity of the employees would constitute a breach of French data protection legislation requiring that all data collected and processed is “adequate, pertinent, and non-excessive in consideration of the purpose for which they are collected.”

If the sole purposes of systems covered by the Standard Authorization must relate to financial, banking, accounting, or corruption violations, the collection of data or facts pertaining to the physical integrity of an employee, for example acts of violence, hazardous premises, etc..., will never be (save for exceptional cases) pertinent to or in line with the strict purpose of the system. This results in the provisions of article 3 being deprived of their meaning and use.

Second, and on a more positive note, the decision confirms the regulatory power of the CNIL. Indeed, the Supreme Court not only based its decision on the legislation, but also on the CNIL standard authorization. This is all the more relevant in that the CNIL recently faced a number of setbacks in the affirmation of its controlling and sanctioning powers in France.

Lionel de Souza is a senior associate in the Intellectual Property, Media, and Technology department in the Paris office of Lovells LLP, where he specializes in information technology law—data protection, e-commerce, and IT contracts. He can be reached at lionel.desouza@lovells.com.
New security breach notification requirements under amended E-Privacy Directive

By Jan Dhont and Katherine Woodcock


The goal of the amended directive is to enhance the protection of individual privacy and personal data via ad hoc amendments that mainly aim at the encouragement of increased information security and enhanced enforcement powers to the competent national authorities of the member states (the authorities). As amended, the E-Privacy Directive introduces an obligation to notify individuals and authorities in instances of information security breaches. The scope of the E-Privacy Directive includes providers of electronic communication services such as telecom operators, mobile phone communication service providers, Internet access providers, providers of the transmission of digital TV content (not the content providers), and other providers of electronic communication services. However, there are indications that this scope could extend beyond this sector, mirroring the U.S. notification requirements. This article will outline the notification regime for breaches of data, the new security obligations, and the new enforcement mechanisms under the amended E-Privacy Directive.

I. Notification requirements

The changes seek to encourage the development of data security via notification requirements in the occurrence of breaches of personal data. Requiring notification encourages accountability, drives investment in data security within provider entities, and allows affected individuals to mitigate their damages. The ability to mitigate the risks associated with security breaches of personal data (e.g. identity fraud, humiliation, physical harm, etc…) is especially important, as it enables affected individuals to take measures to minimize damages. Also, notification requirements could drive competition in the field of data security technology for companies, allowing organizations to identify more effective data protection methods and to eliminate the less effective ones. This may further allow data controllers to assess the practicalities of individual security methods, driving forward the market for data security technology. Many companies perceive that the benefits of notification requirements come at their expense, since it is often embarrassing and tarnishes the public image of companies.

A. Who must notify?

The amendment provides a structure for notifying the competent authorities and individuals concerned when personal data has been compromised. Providers of electronic communication services are required to report security breaches. (Art. 4) There is a distinction between public and private communication service providers; the E-Privacy Directive applies only to providers of public electronic communications networks and services, i.e. telecom operators, mobile phone communication service providers, Internet access providers, providers of the transmission of digital TV content (not the content providers), and other providers of electronic communication services that are offered to the public. (Art. 3) The European legislature explicitly stipulates that the directive “does not apply to closed user groups and corporate networks.” (Recital 55)

It is important to note that the Article 29 Working Party (WP) and the European Data Protection Supervisor (EDPS) already encouraged the broad applicability of notification requirements (i.e. to private providers), due to the impact on citizens irrespective of the sector and the expansion of e-communications to process data. Thus, it is expected that industries that process important quantities of sensitive personal data may be subject to breach notification obligations in the future. The WP, in its opinion dated February 2009, expressed that notification requirements should also be extended to information society services provided by healthcare or financial institutions (e-health applications, e-banking, etc…). The current scope of the notification requirement would, according to the WP, reach a “very limited number of stakeholders” and “would significantly reduce the impact of personal data breach notifications as a means to protect individuals against risks.” Furthermore, the European legislature encourages the expansion, as “interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at community level as a matter of priority.” (Recital 59)

B. Requirements for notification

The providers must give notice on two levels when a personal data breach has occurred. A personal data breach under the amended directive is defined as a
“breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of publicly available electronic communications services in the community.” (Art. 2(h))

The definition is very broad, since a small or initially innocent information security incident potentially constitutes a security breach. Upon breach, the provider must contact the authorities, without undue delay, in order to quickly address the breach and mitigate damages (e.g. economic loss and social harm). Additionally, if such a breach “is likely to adversely affect the personal data or privacy of a subscriber or individual,” then the subscriber or individual should also be notified without undue delay. (Art. 4.3) Awareness of the breach enables the individuals to take necessary precautions and mitigate damages (e.g. cancel credit cards, change passwords, etc...). A breach adversely affects the data or privacy of a subscriber or individual where it could result in identity theft, fraud, physical harm, sign humiliation, or damage to reputation. (Recital 61)

However, the amendment is not clear as to who must make the assessment of the adverse effects on the individual—the authorities or the provider. Individuals do not need to be notified in some circumstances, specifically, when “the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security breach.” These technological measures must render the data unintelligible to any person who is not authorized to access it. This applies to encrypted data and the exception provides that the authorities decide if the providers have implemented sufficient protective measures and need not notify the relevant individuals or subscribers. Further, in cases where the providers have not notified the subscribers, the authorities may require them to do so if, after having considered the likely adverse affects, they deem it necessary. (Art. 4.3) It appears that consultations with the authorities will increase exponentially

See, Breach notification, page 24
and that further clarity will need to be provided by national legislators and authorities.

C. Notice contents and procedures
The notice contents differ depending on the notice recipient, i.e. the authorities or the individuals. The notice to the individual should “at least describe the nature of the personal data breach,” provide a contact point where additional information can be acquired, and should recommend mitigating measures to the possible adverse effects of the breach.” Notification to the authorities should, “in addition, describe the consequences of, and the measures proposed or taken by the provider to address” the breach. (Art. 4.3)

Further, the member states are encouraged to adopt measures delineating the circumstances, format, and procedures for information and notification requirements, granting them increased powers to control the notification process. (See recitals 62-64.) With respect to the rules regarding format and procedures of notification, the council suggests taking into account the circumstances of the breach, including whether the data was protected by adequate security measures. Providers must “maintain an inventory of personal data breaches” with the facts of the breach, effects of breach, and action taken. (Art. 4.4) This is retained and allows for the authorities to verify the providers’ security obligations under the E-Privacy Directive. Audits may take place to see if providers have complied with the inventory of breaches and the authorities may also issue guidelines and instructions with respect to notification. (Art. 4.1a)

II. New security obligations
In addition to the notification requirements, the revised E-Privacy Directive implements new obligations for the security procedures of processing personal data. Additional language requires that providers must take appropriate measures to protect data being processed, including: ensuring such data is accessed only by authorized persons and that the stored and transmitted data is protected against theft, disclosure, or breach. (Art. 4.1a)

Finally, providers must implement a security policy in addition to the existing requirement that they must take appropriate technical and organizational measures to safeguard the security of service and network security. (Art. 4.1a) Such measures should enable the providers “to identify vulnerabilities in the system.” Furthermore, “monitoring and preventive, corrective, and mitigating action should be regularly carried out.” (See recitals 57 & 59.) Such requirements and obligatory implementations portend that providers will keep up with the latest security technologies. Furthermore, providers’ security procedures and corporate actions will evolve with these developments over time.

III. Empowerment of the authorities
In order to facilitate better enforcement and compliance with the E-Privacy Directive, the authorities were granted increased enforcement powers with respect to the security of processing. (See Art. 4.) The council conceives that, in order to promote the interest of citizens, the authorities “should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised.” The authorities should also monitor measures taken to mitigate damages and risks and disseminate best practices among the providers. As the providers must maintain an inventory of personal data breaches, this enables further analysis and evaluation by the authorities. The strengthening of enforcement powers by national authorities allows for the E-Privacy Directive to be more resolutely enforced throughout the EU, although it does leave open the potential for varying national standards.

Finally, new language allows for the member states to provide “penalties, including criminal sanctions, where appropriate, applicable to infringements of the national provisions adopted.” These, of course, would have to be proportionate, but do express stricter entitlements under the reworked E-Privacy Directive.

On a whole, the authorities are granted more power and enforcement mechanisms under the E-Privacy Directive. Further, notification requirements and security policies will force providers to keep up with current data security measures and burgeoning technologies. The expansion in scope of the notification requirements into other sectors is anticipated and encouraged by the European Data Protection Supervisor and WP. This expansion will likely be observed during the implementation of the new directive by the member states in their national legal systems. Such implementation, combined with the possible expansion of notice requirements, could lead to laws that vary widely from member state to member state. This would make pan-European compliance difficult for businesses and it is hoped that the WP will provide timely guidance to enhance a common standard.

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

Katherine Woodcock is an associate at Lorenz Brussels and can be reached at k.woodcock@lorenz-law.com.
Take a tour of our facility, we will be happy to show you the difference.

800-222-2044
www.theshredders.com
CANADA

By John Jager, CIPP/C

CATSA PIA Response

In January, the Office of the Privacy Commissioner of Canada (OPC) released its response to a Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) in anticipation of the deployment of millimetre wave (MMW) screening technology at selected Canadian airports. The adoption of this technology, which shows the outline of an individual’s body beneath their clothing, has been the source of much discussion due to its perceived invasiveness.

The OPC urged CATSA to regularly scrutinize implementation of MMW screening technology and justify it against the following four-part test:

1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the need?
4. Is there a less privacy-invasive way of achieving the same end?

In considering the operational privacy risks of MMW technology, the OPC took into account the 10 privacy principles found in the Canadian Standards Association Model Code for the Protection of Personal Information, which is also included in the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

In response to CATSA’s PIA, the OPC recommended that CATSA:

• develop and publicize a privacy policy about its use of MMW whole-body imaging, which specifically and clearly outlines all privacy management features governing use of the technology
• undertake a public information campaign via its Web site, at airports using posters and brochures, and using other sources such as newspaper or radio announcements, to identify the purposes of the MMW technology to the Canadian public
• ensure the images that are presented in its communications materials, posters and brochures are accurate presentations of the images obtained during MMW screening, in order to ensure informed consent
• clarify the estimated timeframe for the existence of the transitory images
• undertake an IT Threat and Risk Assessment for the system used to transmit images to the Remote Viewing Room for each configuration of MMW units at each airport location, to ensure security of the electronic images and prevent inappropriate use or disclosure

The OPC urged CATSA to use MMW technology only as a secondary screening tool and said the use of MMW should be voluntary, an alternative to undergoing a physical pat-down.

CATSA has implemented a number of steps to ensure that the process is discreet. The operator who sees the passenger at the screening checkpoint will not see the scan, and the official viewing the scan at a remote location will not see the passenger. The process will be anonymous, so that no personal information, such as the passenger’s name, boarding pass number or passport data, will be associated with the image. The images will be viewed for concealed threats and immediately deleted; they will not be recorded or transmitted in any way.

The OPC believes that these measures will help address some of the privacy concerns raised by this new security measure, however it urges CATSA to continue to consider the privacy implications of the technology, and to explore options to further minimize privacy risks for travellers.

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

GERMANY

By Flemming Moos

German DPAs: Web site tracking requires consent

During its November session, the so-called “Düsseldorfer Kreis” (the assembly of all supreme German DPAs) adopted a resolution on the privacy-compliant design of Web site tracking procedures (such as Google Analytics).
In the resolution, the Düsseldorfer Kreis states that an analysis of the Web site usage (including geo-localization) requires opt-in consent of the respective user in case unabridged IP addresses are used for the analysis. The assembly based its finding on the assumption that IP addresses are to be considered personally identifiable information. As a consequence, in the event no proper consent to Web site tracking measures has been secured, all IP addresses would have to be shortened by the last two to three digits before they could be used for any kind of Web site usage analysis.

Yet, even if the IP addresses are depersonalized in the described manner but a certain pseudonym is used that might allow re-identification of the users, further measures would have to be taken, says the Düsseldorfer Kreis, in order to meet the statutory requirements. In particular, the special data protection law provisions of the Telemedia Services Act would require that the users be informed about their right to object even usage profiles created under a pseudonym and that the data are strictly separated from other user data.

Moreover, the assembly points out that the requirements of Sec. 11 of the Federal German Data Protection Act on the lawful creation of data processing agencies must be observed in case a third party is mandated with the analysis.

In another decision adopted on November 27, 2009, the Düsseldorfer Kreis took up the issue of marketers’ data usage. The assembly stated that the recently amended provisions on marketers’ use of personal data provide for a transition period through August 31, 2012 for data that was collected prior to the enactment of the amendment. However, it points out that the new provisions are directly applicable in case the controller cannot prove when the data were first stored.

**Draft law on privacy protection of employees**

The parliamentary group of the Social Democrat Party (SPD) in Germany on November 25 tabled a draft law on privacy protection in employment relationships. The proposal stems from a series of privacy scandals involving German companies illegally spying on their staff.

The draft comprises provisions on (i) the collection of personal data from job applicants and the usage of such data in the application procedure (ii) the possibility of video surveillance and employee location techniques, (iii) data usages related to telecommuting and to employees’ use of Internet and e-mail systems owned by the employer, and (iv) provisions on sharing personal data within groups of companies and the co-determination rights of works councils on privacy issues.

It remains to be seen whether the German parliament will take this draft any further; because the Liberal Democratic Party (FDP) and the Christian Democratic Union (CDU) form the actual government and also hold the majority of votes in both chambers (Bundestag and Bundesrat), it is most likely that they will present their own draft on employee privacy in the course of 2010.

**New data processing agreements: publicly available model clauses**

The recent reform of the Federal German Data Protection Act (BDSG) has brought about significant changes to the requirements data processing agreements must meet in order for transfers between controllers and processors to benefit from the data processor privilege enshrined in Sec. 11 of the BDSG.

According to the revised provisions, data processing agreements must now specify in detail (1) the subject matter and term as well as (2) scope, type, and purpose of the data processing, including the type of data and the affected individuals, (3) the technical and organizational security measures adopted by the processor, (4) obligations to correct, erase, and block the data, (5) control obligations of the processor, (6) possibility of subcontracting, (7) audit rights of the controller, (8) data breach notification obligations, (9) allowed instructions by the controller, and (10) return of storage media and deletion of the data.

As a consequence of this heavily extended minimum content, all existing data processing agreements will need to be revised and adapted to the new requirements. For this purpose, several “model clauses” are publicly available. Inter alia, the DPA of the German Bundesland Hessen, has published respective clauses, which are available (in German) on their Web site (www.rp-darmstadt.hessen.de). Also the German Association for Data Protection and Data Security (GDD) has issued a draft data processing agreement in German (www.gdd.de). Finally, the Federal Association for Information Technology, Telecommunications, and New Media (Bitkom) has crafted a bilingual draft (www.bitkom.org).

Processors and controllers must bear in mind, however, that all these model clauses require adaption to the specific situation. In particular, all model clauses contain appendices—comparable to the EC model clauses for data transfers to data processors—which have to be completed with specific information.

**Hamburg DPA: enforcement actions re obligations to appoint data protection officers**

In a press release dated January 8, the Data Protection Authority of Hamburg announced broad enforcement actions in order to curtail the numerous

See, *Global Privacy Dispatches*, page 28
Due to the fact that German marketing intended recipients have consented, the purchaser shall be obliged to verify whether these consents are documented (e.g. in a written declaration). If a company does not comply with this prior-checking requirement, it might be held responsible for the unsolicited mailings.

The court found that a company that used a government database unlawfully. The second bill would abolish (with minor exceptions) the duty to register databases. The two bills reflect ILITA’s efforts to shift the center of gravity of data protection in Israel from procedural regulation to substantial enforcement.

Flemming Moos is an attorney at DLA Piper in Germany and a certified specialist for information technology law. He chairs the IAPP KnowledgeNet in Hamburg and can be reached at flemming.moos@dlapiper.com.

ISRAEL

By Dan Or-Hof, CIPP

A shift in the regulatory regime

The Information, Law, and Technology Agency (ILITA) held an international conference on data security on January 20 as a means to strengthen data protection in Israel. The conference involved a discussion on ILITA’s recent proposal to enact new privacy regulations related to information security. The proposal aims to subject database owners to information security rules and procedures, including the formation of internal procedures and information security policies, classifications, and privacy risk evaluations in the organizations, encrypting laptops, and more.

Mr. Yoram Hacohen, the head of ILITA, informed attendees of a coming change in the data protection regulatory regime. Within the next few months, two bills will be introduced to amend the Privacy Protection Act (PPA). The first will define and enhance the enforcement capabilities of the database registrar. The bill will provide broad authority to impose fines on organizations and corporations that act in violation of the data protection provisions of the PPA. The bill follows a NIS177,000 (approximately $50,000) fine that was recently imposed by the database registrar on a company that used a governmental database unlawfully. The second bill would abolish (with minor exceptions) the duty to register databases.

Dan Or-Hof is a senior counsel at Pearl Cohen Zedek and Latzer LLP, with specific expertise in data protection and privacy law. He may be reached at dano@pczlaw.com.

UK

By Eduardo Ustaran

Report data breaches or face tougher sanctions

David Smith, deputy commissioner and director of data protection at the UK Information Commissioner’s Office (ICO), has said that organisations reporting their data security breaches may find themselves subject to regulatory action, but “...those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions.” Though it is not a legal requirement to report data breaches, more than 800 organisations have reported breaches to the ICO in the past two years.

According to the ICO, organisations can minimise the risks of security...
breaches involving personal information by ensuring that all portable media devices containing personal information are encrypted. Staff must be adequately trained and organisations should give proper consideration to restricting staff from downloading large volumes of data onto memory sticks and other portable devices.

Up to £500,000 fines for serious breaches
New powers designed to deter data breaches are expected to come into force on April 6, 2010. The ICO will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The power to impose a monetary penalty is designed to deal with the most serious personal data breaches and is part of the ICO’s overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

Code planned for airport scanners
A UK government department is to draw up guidelines for the use of passenger images produced by airport security scanners. The Department for Transport will issue a code of practice for all operators to help ensure that those responsible for the scanning are properly trained and that procedures comply with the Data Protection Act. Prime Minister Gordon Brown recently endorsed the use of full-body scanners at airports, and the British Airports Authority has said it will install the machines as soon as practical, with Heathrow Airport expected to be the first.

Eduardo Ustaran is head of the Privacy and Information Law Group at Field Fisher Waterhouse LLP, based in London. He is a member of the IAPP Education Advisory Board, co-chair of KnowledgeNet London, editor of Data Protection Law & Policy and co-author of E-Privacy and Online Data Protection. He may be reached at eduardo.ustaran@ffw.com.

Calendar of Events

<table>
<thead>
<tr>
<th>APRIL</th>
<th>JUNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>IAPP Certification Testing – Melbourne, Australia</td>
<td>IAPP KnowledgeNet – Paris</td>
</tr>
<tr>
<td>18</td>
<td>14-15</td>
</tr>
<tr>
<td>IAPP Certification Training</td>
<td>IAPP Practical Privacy Series</td>
</tr>
<tr>
<td>Washington, DC</td>
<td>Santa Clara, California</td>
</tr>
<tr>
<td>19-21</td>
<td>21-25</td>
</tr>
<tr>
<td>IAPP Global Privacy Summit</td>
<td>IAPP Delegate Tour</td>
</tr>
<tr>
<td>Washington, DC</td>
<td>Berlin, Brussels, Paris</td>
</tr>
<tr>
<td>21</td>
<td>14</td>
</tr>
<tr>
<td>IAPP Certification Testing – Washington, DC</td>
<td>Privacy After Hours</td>
</tr>
<tr>
<td>3-8</td>
<td>29-1</td>
</tr>
<tr>
<td>APWA Privacy Awareness Week</td>
<td>IAPP Privacy Academy</td>
</tr>
<tr>
<td><a href="http://www.privacyawarenessweek.org">www.privacyawarenessweek.org</a></td>
<td>Baltimore, MD</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
</tr>
<tr>
<td>IAPP Certification Testing – Folsom, CA</td>
<td>IAPP Privacy Dinner</td>
</tr>
<tr>
<td>12</td>
<td>30</td>
</tr>
<tr>
<td>IAPP Certification Testing – St. Louis, MO</td>
<td>Baltimore, MD</td>
</tr>
<tr>
<td>19</td>
<td>26-28</td>
</tr>
<tr>
<td>IAPP Certification Testing – Chicago, IL</td>
<td>IAPP Canada Privacy Symposium 2010</td>
</tr>
<tr>
<td>19</td>
<td>26-28</td>
</tr>
<tr>
<td>IAPP Certification Testing – Dallas, TX</td>
<td>Symposium 2010</td>
</tr>
<tr>
<td>19</td>
<td>28</td>
</tr>
<tr>
<td>IAPP Certification Testing – Denver, CO</td>
<td>IAPP Certification Testing – Toronto, ON</td>
</tr>
<tr>
<td>26-28</td>
<td>28</td>
</tr>
<tr>
<td>IAPP Canada Privacy Symposium 2010</td>
<td>IAPP Certification Testing – Toronto, ON</td>
</tr>
<tr>
<td>28</td>
<td></td>
</tr>
<tr>
<td>IAPP Certification Testing – Toronto, ON</td>
<td></td>
</tr>
</tbody>
</table>

To list your privacy event in the Privacy Advisor, e-mail Tracey Bentley at tracey@privacyassociation.org
Indiana University hosted a full day of Data Privacy Day events, featuring speakers on privacy topics such as FERPA, HIPAA, and social networking. IU Chief Information Policy Officer Merri Beth Lavagnino said about 200 people attended the event, with some trickling over to the IAPP Privacy after Hours event at Farm Bloomington (below).

Privacy pros celebrated Data Privacy and Protection Day at events across the globe on January 28.

During her Data Protection Day keynote speech at the European Parliament, EU Justice Commissioner Viviane Reding said, “It is my firm belief that we cannot expect citizens to trust Europe if we are not serious in defending the right to privacy. We need to ensure that personal data are protected against any unauthorized use and that citizens have the right to decide on the way their data are processed.”
Ontario Premier Dalton McGuinty stands with Ontario Information and Privacy Commissioner Ann Cavoukian before opening the ceremonies at the Second Annual Privacy by Design Challenge in Toronto on Data Privacy Day. Commissioner Cavoukian hosts the annual challenge.

(Right) After hours fun for privacy pros in the Texas capitol. LtoR: Vanessa Hayward; Julie Ferguson, Debix; Kathy Carsno, Dell Financial Services

(Below) LtoR in Austin, Texas: Vanessa Hayward; Erin Fonte of Cox Smith; Austin Knowledge co-chair Mike Wyatt of Deloitte; Hunter Dodson of Dell; Privacy After Hours hostess and Austin KnowledgeNet co-chair Alison Brunelle of Dell.

A “series of lively conversations” dominated the Los Angeles Privacy after Hours gathering, according to host Ozzie Fonseca, CIPP, of Experian Consumer Direct.

Privacy pros gathered after hours in Seattle, Washington on Data Privacy Day.
Improving information security risk management and data leakage prevention (DLP) are the top two priorities for the year ahead, according to Ernst & Young’s 12th annual global information security survey. Compiled from the responses of information security professionals from nearly 1,900 organizations based in locations across the globe, the survey also lists regulatory compliance as a key goal among respondents. However, the report states, “too few organizations have taken the necessary steps to protect personal information.”

The survey shows that while “authorized users and employees pose the greatest security threat to an organization” and the majority of respondents do have security awareness programs in place, less than half—44 percent—of those programs include updates and alerts on current threats, while 42 percent provide informational updates on key new topics and 35 percent present specific awareness activities for “high-risk groups such as social networking users.”

According to the survey:

- 68 percent of respondents understand privacy laws and regulations
- 63 percent “include privacy requirements in contracts with external partners, vendors, and contractors”
- 59 percent have implemented specific controls to protect personal information
- 32 percent of respondents have produced an inventory of information assets covered by privacy requirements
- 29 percent have implemented a process to monitor and maintain privacy controls
- 26 percent have conducted assessments of the life cycle of their personal data

However, when it comes to personal information, the report points out that:

- 50 percent of respondents are at some stage of the evaluation and implementation process for DLP security technology, the survey also shows areas of concern. “One of the most noteworthy survey findings is how few companies are encrypting their laptops,” the report states, with only 41 percent of respondents currently using encryption and 17 percent planning to do so within the next year.

The report points out that many breaches have occurred and continue to occur due to the loss or theft of laptop computers. “The technology is readily available and affordable to implement,” the report states, while having a “relatively low” impact on users as it is put into place.

While 50 percent of respondents are planning to implement virtualization by the end of the next year; however, just 19 percent of those responding organizations listed virtualization as a security priority. “Clearly, our survey respondents do not recognize the same level of risk with virtualization as would be expected with such significant and extensive change effort,” the report states. “More alarming is the fact that virtualization security should be a concern, but the majority of organizations and security leaders are ignoring its implications.”

Cloud computing does not have as much push yet as virtualization, according to the responses, with only 17 percent indicating they now use the technology or plan to do so within the next year.

“Coupled with the opportunities and promise of cloud computing are elements of risk and management complexity. There are many challenges regarding types of cloud computing and the scope of deployment that make the details not nearly so simple,” Amr Ahmed, senior manager in Ernst & Young’s Advisory Assurance practice, told Privacy Advisor.

Ernst & Young identifies those challenges as:

- Data management at rest and in transit—privacy, regulatory violation, legal implication, cloud contract termination
- Security vulnerability within the infrastructure—authentication, authorization, access control, cryptography, monitoring
- The threat of “Monoculture”—diversity, resiliency, disaster recovery, and business continuity
- Service-Level Agreements—whether vendors offer flexible, negotiated,
In our continuing series to celebrate the IAPP’s 10-year anniversary, this month we look back at the early days of the privacy profession with Jennifer Barrett. Widely considered the first person to hold the title of chief privacy officer, Jennifer has been heading up privacy efforts at Arkansas-based databroker Acxiom Corp for almost 20 years. Jennifer joined Acxiom in 1974 after receiving a degree in mathematics and computer science from the University of Texas at Austin, and prior to her position as CPO worked in almost every facet of the company. The Privacy Advisor asked her a few questions about her work, and how it has evolved through the years.

**What were some of the things you were concerned with during that first year as CPO?**

In 1991 when I first took on the role of CPO there was no general privacy related legislation domestically or in the UK which at that time was our only international operation. There were emerging concerns about telemarketing and a few state do-not-call registries, the first one having been enacted in Florida in 1986. My CPO responsibilities only took up about 25 percent of my total time and were focused on improving the DMA self-regulatory guidelines for telemarketing and direct mail. Credit issuers were a large segment of our client base, so we also complied with the FCRA guidelines relative to pre-approved offers of credit. All in all, a pretty simple world compared to today.

**What are some of the biggest changes you’ve seen since the beginning of your career in privacy?**

My entire career has been managing through one big change after another. This includes an explosion of laws, regulations, and industry codes of conduct coupled with some extraordinary corporate growth at Acxiom. When I took on the role of CPO we were only doing business in three countries—the U.S., Canada and the UK. Now we offer some services that are worldwide and have offices in 14 countries. In the beginning we only offered marketing-related products and services. Now we have a whole line of risk and identity management products and services for clients in industries ranging from financial, insurance, telecommunications, technology, retail, catalog, publishing, travel and entertainment to government. Revenues have grown tenfold in the last 19 years and I’ve had almost that many bosses. One of the biggest challenges I’ve had (and, I think, any other CPO with global responsibility has) is keeping up with the evolution of all the various risks associated with these new technologies.

To read the full report, visit www.ey.com/Publication/vwLUAsset/s/12th_Annual_Global_Information_Security_Survey/$FILE/12th_annual_GISS.pdf.

—Jennifer L. Saunders
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 December 2009:

William David Alfveby, CIPP/IT
Wesley Howard Avery, CIPP
Allen Balasa, CIPP
Bharanedaran Balasubramanian, CIPP
Ngoc Thuy Teri Barnett, CIPP/G
Wanda Bell, CIPP
Eric E. Breisach, CIPP
Venyssa Naomi Brown, CIPP
Miriam M. Brown-Lam, CIPP/G
Anne Cristina Burbach, CIPP
Dorothy Julia Clarke, CIPP
Matthew James Daley, CIPP
Benjamin Michael DeMaria, CIPP/G
Marcia Shea Dixon, CIPP/IT
Jaemie Leah Drake, CIPP/G
Patricia Allen Farrie, CIPP/G
Anne Clifford Foster, CIPP
Wesley Tyler Fravel, CIPP/G
Marsha Goldberger, CIPP
Philip McKinley Greene, CIPP
Meredith Britt Halama, CIPP
Donald K. Hawkins, CIPP/G
Amanda B. Hopper, CIPP
Lauren Jennifer Jarvis, CIPP
Arthur A. Johnson, CIPP/G
Elimu Etumba Kajunju, CIPP/IT
John W. Kelley, CIPP
Kevin J. Kelley, CIPP/G
Gary Kibel, CIPP
David Gebhart Krone, CIPP/G
Sonia Lanteigne, CIPP/C
Grace Lewis, CIPP
Natasha Hadia Martin, CIPP
James Richards McEvoy, CIPP
Shawn Mewhorter, CIPP/G
Gloria Nella Muscardin, CIPP
Nancy Warren Northrup, CIPP
Bridge Lynn O’Connor, CIPP
Susan T. Pouget, CIPP/G
Edo Raday, CIPP
Richard Russell Reynolds, CIPP
Kristy Sterrett Sawyer, CIPP/G
Jeffrey S. Scehnet, CIPP/G
Brandon Joel Schneider, CIPP/G
Alex Shojay, CIPP/G
Steffani Amber Smith, CIPP/G
Meredith Regina Snee, CIPP/G
Walter Tamminen, CIPP
Suzanne Keir Yurk, CIPP

Did You Know?

Listomania
The IAPP recently combined its seven industry-specific listservs into one comprehensive list—the Privacy Listserv. Already very active, privacy pros are discussing topics ranging from the masking of Social Security numbers to logical data separation and social media policies. Have a question? Pose it to your peers on the listserv.
www.privacyassociation.org/community/privacy_listserv/

Privacy advisors
The fiscal 2011 budget for the U.S. Department of Health and Human Services proposes $1.6 million for the Office of Civil Rights for “regional privacy advisors.”
Source: InformationWeek

Define “friend”
A survey of 1,150 British youngsters revealed that 25 percent have hacked or attempted to hack their friends’ Facebook accounts for fun. Twenty-one percent admitted that they hoped to cause disruption, but most of the would-be hackers failed. The study found that 82 percent did not succeed in their tampering endeavors.
Source: Fast Company
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.

EU PRIVACY MANAGER AND OFFICE MANAGER
eBay
Luxembourg, Luxembourg

PRIVACY RESEARCH ANALYST
Highmark Inc.
Pittsburgh, PA or Camp Hill, PA

PROGRAM MANAGER
TRICARE Management Activity Privacy Office Support
Falls Church, VA

PRIVACY ADVISOR
Highmark, Inc.
Pittsburgh, PA

SR. CORPORATE COUNSEL, GLOBAL PRIVACY OFFICE
Pfizer
New York, NY

PRIVACY MANAGER
University of Florida
Jacksonville, FL

MANAGER – SUBSCRIBER PRIVACY & DATA SECURITY
Cablevision
Bethpage, NY

DIRECTOR, INFORMATION PROTECTION AND PRIVACY
Marriott International
Maryland

INFORMATION SECURITY OFFICERS
The World Bank
Washington, DC

PRIVACY PROJECT MANAGER
Genentech
South San Francisco, CA

In the Privacy Tracker this month...

Earn CPE credits

Looking for a way to earn IAPP Continuing Privacy Education credits tailored to your business? Subscribers to Privacy Tracker earn automatic credit for dialing-in to the monthly audio calls tailored to your coverage requests. Earn up to 12 CPE credits each year!

Are you an expert in your privacy sector and want to author an article on a timely issue with a legal or legislative focus? Send us a proposal to privacytracker@privacyassociation.org.

Privacy Tracker keeps you up to date on all federal and state privacy legislation. Subscribers receive weekly e-mails highlighting privacy bills on the move and monthly audio calls tailored to their coverage requests. Privacy Tracker subscribers also enjoy exclusive access to feature stories and expert commentary on the latest legislative privacy developments.

Subscribe today!

www.privacytracker.org

The Lighter Side of Privacy

Reprinted with permission from Slane Cartoons Limited.
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

Privacy News

Rutherford to chair this year’s PCI council

Bruce Rutherford, head of MasterCard’s fraud management solutions, payment system integrity group, will serve as this year’s chairperson of the Payment Card Industry (PCI) Security Standards Council.

Under Rutherford’s leadership, the council will release new standards to enhance payment account security and awareness in 2010. Additionally, Rutherford will work with the council’s board of advisors, participating organizations, assessor community, and merchants to increase adoption of PCI standards.

“This next year will be crucial for developing the ongoing practices and disciplines necessary for the security of payment card transactions,” says Bob Russo, general manager of PCI Security Standards. “I look forward to working closely with Bruce and the rest of the council’s stakeholders to continue to improve payment security globally.”

—Angelique Carson