Privacy as a competitive differentiator

In front of a packed hall at an OECD conference in Jerusalem last month, one of the world’s foremost experts on information privacy dismissed the idea of companies using privacy as a competitive differentiator. During a panel session featuring some of today’s most highly regarded data protection experts and regulators, Alan Westin said the idea that privacy can be used as a business advantage is dead, privacy controls are too complex for consumers to understand and a certification culture would be more effective.

His comments came just a few months after we first heard of Diaspora, the new social network that hopes to compete on privacy, and a slew of other new companies that are banking on their privacy focus, such as RockMelt, the new social Web browser that will not house ads because its founders believe to do so would diminish users’ privacy.

"You can't have a good user experience if somebody is (taking) your data and using it to sell ads," RockMelt co-founder Tim Howes told The Wall Street Journal.

What do you think? Does your company distinguish itself on its privacy-related merits? Do you shop around on privacy? Let us know.

Sincerely,

J. Trevor Hughes, CIPP
President & CEO, IAPP
International data protection laws

By Miriam Wugmeister and Cynthia Rich

In the past year, two more countries in Asia—Malaysia and Taiwan—have adopted comprehensive national privacy laws that regulate the collection, use and disclosure of personal information. These new privacy laws differ considerably from those in the United States. U.S. laws typically focus on addressing misuse of information and seek to protect individuals from particular harms. These two laws, instead, are omnibus laws that extend protections to all personal information and focus not only on the use of information but also on the collection and disclosure of personal information. With the addition of these two new international laws, there are now almost 80 countries with comprehensive privacy laws in effect, many of which have their own unique regulatory requirements. The addition of each new foreign law poses greater compliance challenges for global organizations. This article provides an overview of the requirements contained in the data privacy laws recently adopted in Malaysia and Taiwan.

MALAYSIA

Overview

The Personal Data Protection Act 2010 was given Royal Assent and published in the Gazette on June 1, 2010; however, the act will only come into operation on a date determined by the minister of information, communication and culture. No date has been set, but the Personal Data Protection Commission is expected to be set up by the end of 2010 or beginning of 2011. Implementing regulations will then need to be issued. Once the act enters into force, private sector organizations will have three months to comply.

This act establishes comprehensive rules for the processing of any personal data “by private sector entities in respect of commercial transactions.” Commercial transactions are defined as “any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2009.” One key question for organizations is whether this act will apply to the processing of employee data. Until the Malaysian Act enters into force and guidance is issued by the regulatory authority, this question will remain unanswered.

The act will apply to all other data processing by private sector entities that are established in Malaysia or, if not established in Malaysia, use equipment in Malaysia for processing personal information. The act does not apply to Malaysia’s federal and state governments.

Definition of Personal Information
Personal information includes any information with respect to commercial transactions that relates “directly or indirectly” to a data subject, who is “identified or identifiable from that information or from that and other information in the possession of” the data user (data controller). This includes sensitive personal information, which is defined as personal information relating to the physical or mental health or condition of a data subject or his or her “political opinions, religious beliefs or other beliefs of a similar nature.”

**Notice**

A data controller must provide data subjects with a written notice that advises them that their personal information is being processed and provides them with a description of that information, the purposes for which it is being processed, the class of third parties to whom their personal information may be disclosed and the source of the personal information. In addition, the notice must explain the data subject’s access and correction rights, the way to contact the data controller with any inquiries or complaints, the choices and means the data controller offers for limiting the processing of the data subject’s personal information, whether it is obligatory or voluntary for the data subject to provide the information and the consequences if the data subject refuses to provide the personal information.

Notice should be given as soon as “practicable” by the data controller, which could mean when the data subject is first asked to provide the information or when the data controller first collects the personal information. The notice must be given, however, before the data collector uses the personal information for a purpose other than the purpose for which the personal information was collected or before the data collector discloses the personal information to a third party.

**Consent**

Subject to limited exceptions, explicit consent is required to process sensitive information; consent (undefined) is required for non-sensitive information. A data subject may withdraw consent by providing the data controller with a written notice stating the objection to the processing of personal information. In addition, a data subject may, at any time by written notice, require data controllers to cease or to not begin processing personal information for direct marketing purposes.

The exceptions for the processing of sensitive data contained in the Malaysian act are similar to those found in many European laws. For example, consent is not required where processing is necessary to protect vital interests, obtain legal advice, administer justice, or provide medical care. In addition, consent to process sensitive data is not required in order “to exercise or perform any right or obligation permitted or required by law in connection with employment.” This latter exception suggests, despite the previously discussed ambiguity about whether the processing of employee data falls within the scope of the act, that employee data may in fact be covered; however, until the authorities issue guidance, the full scope of the law remains unclear.

Finally, consent to process non-sensitive personal information is not required if the information has been made public as a result of steps deliberately taken by the data subject.

**Data Security**

The data controller must take “practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.” A variety of factors such as the nature of the personal information and the harm that could result from such a misuse of the personal information should be taken into account when adopting security measures. Where personal information is to be processed by a data
processor, the data controller must ensure that the data processor provides sufficient guarantees regarding the security measures it will take and must supervise compliance with those security measures.

**Data Integrity**

The data controller must take reasonable steps to ensure that the personal information is accurate, complete, not misleading and up-to-date for the purposes—including any directly related purpose—for which the data was collected and further processed.

**Data Retention**

In addition, the data controller must ensure that all personal information is destroyed or permanently deleted if it is no longer required for the purpose for which it was collected.

**Access and Correction Rights**

Subject to certain exceptions, data subjects must be given access to their personal information held by a data controller and be able to correct that personal information where inaccurate, incomplete, misleading or not up-to-date. Access requests are to be made in writing, and a fee may be charged for such requests. The data controller must keep and maintain a record of such requests; the personal data protection commissioner may determine the manner and form in which the record is to be maintained.

**Data Transfers Outside of Malaysia**

A data controller may not transfer any personal information to a place outside Malaysia unless the jurisdiction is listed in a notification issued by the minister of information and published in the Gazette, or an exception applies. The approved jurisdictions must have in place laws that are substantially similar to the Malaysian act or must ensure an adequate level of protection that is at least equivalent to the level of protection afforded by the Malaysian act.

Alternatively, transfers to places outside Malaysia may occur if one of the listed exceptions applies. Some of these exceptions are similar to those found in European laws, such as the data subject has consented to the transfer; the transfer is necessary to carry out a contract between the data controller and the data subject; the transfer is necessary to conclude or carry out a contract between the data controller and a third party at the request of the data subject, or the transfer is in the interests of the data subject.

Transfers outside of Malaysia will be permitted in cases where the data controller “has taken all reasonable precautions and exercised all due diligence to ensure the data will not, in that place, be processed in any manner which, if that place is Malaysia, would be a contravention of this act.” Further guidance from the regulatory authority is needed, however, to clarify what measures will satisfy the conditions set forth in this exception.

**Database Registration Requirements**

While the Malaysian act establishes detailed registration requirements, it does not specify to whom such obligations would apply; rather, it gives the relevant minister the authority to designate a class of data controllers that will be required to register under the act. Consequently, until the regulatory authority is established, it remains unclear which types of organizations, if any, will be subject to registration obligations.

**Penalties**
Violations of the Malaysian act, such as unlawful processing of sensitive personal information, transfers to jurisdictions not approved by the minister or failure to honor a request to cease processing, can result in up to two years of imprisonment, a fine up to 200,000 ringgit or both. Unlawful collection, disclosure or sale of data is punishable by imprisonment up to three years, a fine up to 500,000 ringgit or both.

TAIWAN

Overview

In 1995, Taiwan adopted a Computer Processed Personal Data Protection Act (the CPPDPA). That law covered data in specific sectors such as financial, telecommunication and insurance and only covered computerized data. In April 2010, Taiwan amended that law with the Personal Data Protection Act (the PDPA). The PDPA now provides protection to personal data across all public and private entities and across all sectors.

The PDPA will only become effective when the Executive Yuan, the central government administrative authority, issues an official order that specifies its effective date. According to government authorities, the PDPA should become effective by November 2011.

Definition of Personal Information

The PDPA has expanded the CPPDPA definition of personal information to include not only computer-processed personal information but also personal information in any data format. Personal information now includes any information that refers to a "natural person's name, date of birth, national unified ID card number, passport number, characteristics, fingerprint, marital status, family, education, occupation, medical history, medical treatment, genetic information, sex life, health examination, prior criminal records, contact information, financial status and social activities as well as other data which can be used directly or indirectly to identify" this natural person.

Collection Limitations

Unlike the CPPDPA, which does not forbid the collection or use of any specific kind of personal information, the PDPA prohibits anyone from collecting, processing or using sensitive personal information except in very narrow circumstances. Sensitive personal information is defined as medical treatment, genetic information, sex life, health examination, and prior criminal records. In particular, sensitive personal information may only be processed when explicitly required by law; necessary to carry out a statutory obligation, and only provided appropriate security measures are in place; made public by the data subject or through other legal methods, or carried out by a government agency or academic research institute for medical purposes, crime prevention, research or statistical purposes. The PDPA authorizes the central competent authorities and the Ministry of Justice to develop regulations regarding the processing of sensitive information.

The collection limitations on non-sensitive information remain largely the same as under the existing law. In particular, non-sensitive personal information may be collected and processed only for a specific purpose, when, for example, the information is explicitly required by law; the private sector organization is engaged in a contractual or quasi-contractual relationship with the data subject; the written consent of the data subject has been obtained, or the personal information has been made public by the data subject or through other legal methods. In addition, personal information may be used for a different purpose but only when, for example, the information is expressly required by law; necessary to avoid danger to the life, body, freedom or property of the
data subject or to prevent serious damage to the rights and interests of others, or the written consent of the data subject has been obtained.

Notice

Subject to certain exceptions, notice must be provided to data subjects when personal information is collected from them and must include information such as the name of the entity that is collecting the information, the purposes of collection and use, the type of information to be collected and the duration of use of the information. Data subjects must also be informed of their access and correction rights. If personal information is not collected directly from the data subject, notice must be provided to the data subject prior to processing or using, and the data subject must be advised about the source of the personal information being collected.

Consent

Where consent is to be obtained, it must be in writing and only after the requisite notice has been provided. If personal information is to be used for a different purpose than described in the notice, and consent will be used as the legal basis for this new use, then a separate written consent must be obtained from the data subjects after they have been expressly informed about the different purpose and the effect their consent or refusal will have on their rights and interests.

Data Security

Private sector organizations that hold personal information are required to adopt appropriate security measures to prevent information from being stolen, altered without authorization, destroyed, eliminated or divulged. The competent authority responsible for regulating a specific industry may require organizations subject to its oversight to develop data security maintenance plans or data disposal procedures.

Data Integrity

Private sector organizations must maintain the accuracy of the personal information, supplementing or correcting the information on their own initiative or upon request from the data subject.

Data Retention

When the purpose of collection has been fulfilled or the period in which the personal information may be used has expired, the private sector organization must delete or discontinue processing the information, or it must delete the information when requested to do so by the data subject, unless the processing or use is necessary to perform a business operation or a written consent of the data subject has been obtained.

Access and Correction Rights

Subject to a number of exceptions, a data owner whose personal information has been processed has the right to access, review, receive duplicates of, cancel the collection, processing or utilization of, and delete the personal data. These rights cannot be waived in advance or limited by an agreement. The PDPA requires that access requests be acted on within 15-30 days. Correction requests must be acted upon within 30-60 days. Organizations may, at their own discretion, charge a fee to cover the costs associated with responding to such requests.

Data Transfers Outside of Taiwan
There are no explicit cross-border restrictions contained in the amended law; however, the PDPA does give government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions, such as when the transfer involves a major national interest, there are special provisions in an international treaty or agreement restricting the transfer, the receiving country does not yet have proper laws and regulations to protect personal data so that the data owner’s rights and interests may be damaged and personal data are indirectly transmitted to a third country to evade this act.

Database Registration Requirements

Under the CPPDPA, organizations had the obligation to file a registration and obtain a license. The PDPA abolishes the CPPDPA’s previous registration requirements, and there are no obligations to file registration with any authority.

Breach Notification

In the event that the data controller has violated provisions of the PDPA, causing personal data to be stolen, divulged or altered without authorization, or infringed upon in any way, the data controller must notify the data subject after an investigation has been completed.

Penalties

The PDPA significantly strengthens the penalties that can be imposed on organizations that violate the law. For example, organizations that profit from the collection, processing, or use of personal data can be fined up to NT$1 million—compared to NT$40,000 under the CPPDPA— or face a term of imprisonment of up to five years versus two years under the CPPDPA. Depending on the gravity of the violation, damages of NT$500-2,000 may also be claimed per violation of the PDPA even if the actual damage cannot be proven. In addition, class action suits will be permitted.

IMPLICATIONS

The new laws in Malaysia and Taiwan significantly change the privacy landscape in these countries. Organizations should carefully examine their existing data privacy practices and procedures to ensure they comply with these new laws. Failure to comply with these laws can result in significant civil and criminal penalties.

For many organizations, it will mean that in these countries, they will have to issue privacy notices, obtain consent to process, use and transfer personal information, establish mechanisms for individuals to exercise their access and correction rights and ensure that their data security and retention policies and practices conform to the laws’ requirements. In addition, organizations in Taiwan will now have an obligation to notify individuals in the event of a data security breach.

Moreover, in both countries, organizations may be subject to specific cross-border limitations, which will further complicate their efforts to transfer and share data within their global organizations. Consequently, they may have to establish new legal mechanisms to enable such transfers to continue. Organizations also need to examine their data collection practices, particularly in Taiwan, to ensure that their practices comply with the collection limitations set forth in the law.

Organizations should assess their data privacy practices and procedures in Malaysia and Taiwan and begin to formulate compliance plans, bearing in mind, however, that it will be difficult to finalize compliance efforts until
these laws become fully effective and implementing regulations and regulatory guidance are issued by the authorities.

*Miriam Wugmeister is a partner in the New York offices of Morrison Foerster LLP and is chair of the firm’s Global Privacy and Data Security Group.*

*Cynthia Rich is a senior international policy analyst in the Washington office of Morrison & Foerster LLP and is a member of the firm's international Privacy and Data Security Practice.*
Poland’s data protection outlook: A conversation with the inspector general for personal data protection

By Angelique Carson

Poland is in the process of amending its 13-year-old data protection law. Inspector General for Personal Data Protection (GIODO) Wojciech Rafał Wiewiórowski, who was elected last July, spoke with the Privacy Advisor about the data protection challenges facing Poland, including the speed at which technology develops and the struggle to keep pace legislatively. Wiewiórowski says he envisions Poland playing a leading role in the changes to EU data protection laws and discusses the key issues filling his schedule at present, including working with stakeholders and government on the future implementation of the smart grid and working with the direct marketing industry on a best practices code.

Not the Wild West, but work to be done

Poland’s Data Protection Act has been in effect since 1997, which, Wiewiórowski says, gives Poland a 13-year foundation in data protection within a European context. “We are not the Wild West or the wild east as far as data protection is concerned,” he says. However, Wiewiórowski says the privacy laws used to govern the Internet are now outdated, and tools from the twentieth century are being applied to twenty-first century technologies, which he compares to trying to fit a square peg through a round hole. The law must catch up with advances in technology, he says, with an understanding that technology will continue to advance.

“That is the challenge for the legislature in Poland; that is the challenge for the lawmakers,” he says. “We know that even if we catch the things we want in 2010, in 2013 the world will once again look a bit different.”

Data sharing problematic

According to the commissioner, closing the gap between emerging technologies and legislation will require some significant work, as legislative action is at a nascent stage in Poland. In the meantime, there are existing problems to be resolved, such as the amount of data kept by Poland’s secret services and the electronic sharing of information through the Stockholm Programme, which was passed last year by the European Council and establishes rules for cross-border sharing of police databases in the EU. He says that while European programs move toward electronic records on the basis of free data flow for all European countries, neither the legal nor the organizational environments in the EU are prepared.

“From the perspective of the police, this is very interesting and useful. But creating such a system for all 27 countries of the EU is quite a challenge for authorities because the authorities of one country will have access to very sensitive data that may be in the hands of another country in the EU. “So we have to be careful to deal with it in the right manner,” he says. “For us, that’s a huge challenge.” Wiewiórowski adds that the new framework allows for much broader information sharing than the former framework, the Hague Programme, which expired in 2009.

New services such as Google’s Street View are also poised to create data protection and privacy problems in Poland’s near future. Warsaw Business Journal recently reported that Wiewiórowski is checking the legality of the service, and the commissioner told the Privacy Advisor, “We are looking at the problems that have arisen in
countries like France, Germany and the Czech Republic and are waiting for the problem in Poland. We're trying to be prepared.”

Major changes expected to privacy law

Poland began amending its data protection law in 2009, and it is expected to be complete by the end of 2011. Wiewiórowski says the law aims to regulate more than is typically included in privacy law by adding sector-specific language, including that related to the medical and banking sectors and the new EU regulations on maritime passengers.

“There is huge work to be done in the next year and a half and then the legal procedure in parliament,” Wiewiórowski said. Noting Poland’s geographic size and that it is “quite a huge part of the European market,” he says he would like the nation to be one of the main actors in changes to data protection law across the European Union, which EU Commissioner Viviane Reding has said will be “significant.”

Best practices code

Wiewiórowski points to recent negotiations with the direct marketing industry as evidence that data protection authorities can work with industry to find solutions acceptable for both sides of the room.

“Cooperating with the direct marketing industry in Poland is one of our benchmark solutions,” Wiewiórowski says, adding that his office is promoting a best practices code to be implemented within the Chamber of Commerce and involving sector-specific organizations.

There have been ongoing problems with the direct marketing sector in Poland for the last 10 years, Wiewiórowski says, but they are meeting in the middle.

“We have proposed an ethical code and what the best practice code should look like,” he said. “We started a war with them 10 years ago, and now we have practical cooperation on a day-by-day basis. So this is the benchmark we give to other sectors. We say, listen, even with such a difficult sector like direct marketing, we can find good solutions that are acceptable both for them and the data protection authorities.”

Wiewiórowski said there are still complaints about the direct marketing industry, but it’s useful to show other industries the progress that’s been made on the best practices code in terms of how problems can be solved. He cites recent success working with the Catholic Church to create the best practice code “Guidelines on Personal Data Protection in the Activity of the Catholic Church in Poland.” Bishop Stanisław Budzik signed the guidelines, which explain obligations imposed on the data controller in pastoral work and note Internet risks.

“It may work. You can do it even with such a traditional sector like the Catholic Church,” Wiewiórowski says.

The smart grid

According to the commissioner, the smart grid is also a concern to be addressed. Grid adoption is about seven years away in Poland, and it is on Parliament’s radar, but Wiewiórowski says he’s concerned that various sectors, including lawyers and data protection professionals, don’t yet understand the ways the smart grid could affect them and the average citizen in the future. He says, however, that Poland has so far done a good job of involving data protection authorities early on in the smart grid planning stages, which pleasantly surprised him. “The data protection authorities have been invited to the discussion from the very beginning,” he said, allowing for privacy
and data protection issues to be found early and solved “together, with the data protection authority, not against or apart from it.”

Read more by this author:

How will privacy apply to apps?

Smart grids are the future of power, but what does that mean for the future of privacy?

Global Privacy Enforcement Network aims to facilitate cooperation

Close-up on COPPA at FTC Roundtable

Schools team with ICO to tech Internet safety
Cloud computing: Value proposition and risks

By Miranda Alfonso-Williams, CIPP, CIPP/IT

This is the second article in a three-part series on cloud computing. View the first installment in the November issue of the Privacy Advisor.

Overview
The first installment of the cloud computing series provided an overview of cloud computing and practical examples of the ever-evolving phenomenon. This article discusses the value proposition that can be derived from cloud computing and some of the privacy risks that should be considered before moving into the cloud.

Economists have compared the current state of the economy to that of the Great Depression. In the midst of this storm, business leaders face shrinking budgets, headcount reductions, pressures to reduce costs and the need to do more with less. They are consistently challenged to identify opportunities that increase the bottom line and improve overall efficiency.

Benefits/value proposition
Cost savings is a major benefit derived from cloud computing. When exploring cost savings, leaders should consider some of the benefits that can be gained by shifting from the traditional data center model to some of the options available in the cloud. The cost to retrofit a datacenter with infrastructure, hardware, storage systems, environmental controls and redundancy can be exorbitant. Cloud providers offer an array of services that can replace many of the activities that are performed within a data center.

As discussed in the first part of the series, the cloud offers the following options:

1) Software as a service (SaaS)

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor and made available to customers over the Internet. SaaS works as a "pay-as-you-go" model. Salesforce.com is an example of this type of offering. Salesforce.com offers a Customer Relationship Management (CRM) product that provides sales people with a single repository to track information about their customers. The shift to the cloud provides a single database to track sales activity, account history, contacts, customer profiles, conversations and more. Increased productivity, sales conversions and identifying future prospects are just some of the value added benefits that can be obtained from the move to the cloud. Automatic Data Processing (ADP) is another example of SaaS; many companies utilize ADP to process their payroll. With the trend of employees being asked to do more with less, moving to the cloud can present companies with the opportunity to focus more on core competencies and utilize their staff more efficiently.

2) Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is similar to SaaS in that a product is offered via the Internet to a client as an on-demand service, but instead of software, IaaS delivers hardware such as servers, network equipment, memory, CPUs and disk space as a service. Amazon.com is a brand that is synonymous with electronic commerce. Amazon has transformed its business model from a premier online seller of books online to general retail. They have, once again, reinvented themselves and become industry leaders in the cloud computing space. Amazon offers a virtual
computing environment called Amazon Elastic Compute Cloud (Amazon EC2); users have the ability to build a virtual computing system based on their requirements.

3) Platform as a service (PaaS)

Platform as a Service (PaaS) solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through a browser. With PaaS, developers can build Web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills. Google’s App Engine is one of the most prominent examples of platform-as-a-service cloud offering. App Engine provides a single, pre-built solution for constructing very large scale Web-based applications hosted on Google’s infrastructure.

During the 1990s outsourcing was the big “boom.” The “cloud” is poised to be the big “bang” of the twenty-first century. The passage of the HITECH Act has positioned the healthcare industry for the transition into the cloud. The transformation from paper records to electronic medical records (EMRs) offers an array of benefits for patients and clinicians. Improved quality of care, comprehensive information about the patients’ medical history and access are a few benefits. Before moving into the cloud, it is imperative that due diligence is conducted to ensure that data is properly secured and protected.

What are some of the risks?

For privacy practitioners, the following are some risks that should be evaluated and mitigated.

Regulatory landscape

The regulatory landscape presents significant challenges when operating in the cloud. The very nature of the cloud makes it challenging to know where data is located at any given time. That said, data can be in multiple states and multiple countries. This loss of control or traceability can have significant consequences depending on the type of data. The HITECH Act protects patient data. Breach notification is a requirement under the act. But, how do we know if a breach has occurred if we do not know where the data is located at all times? The EU Directive also has very clear guidelines on how personal data should be handled and processed. How do we ensure that this occurs in the cloud? Other legal considerations: What do we do when we are faced with conflicting laws? If data is stored in multiple locations throughout Europe, what jurisdiction has preference?

The cloud provider location has significant regulatory ramifications. If a cloud provider is located in Europe and the data is being processed or transferred to the U.S., this type of transfer would be a violation under the EU Directive. Given the sectored nature of the privacy laws, the U.S. is not deemed to have adequate privacy practices.

When asked about some of the regulatory challenges, GE Chief Technology Officer Gregory Simpson stated, “Initially, you may have to target specific geographic regions (eg: a U.S. cloud, an EU cloud)...legislation is way behind the technology capability at this point.”

Although the idea of moving to the cloud has a lot of appeal and potential opportunity, there are still many unknowns. Cloud providers must be able to ensure that data is truly secure. As the regulatory landscape continues to evolve, legislation will eventually catch up with some of the technological advances. Regulators around the
globe are aware of some of the challenges and many are actively developing guidelines that will ensure that data is handled adequately.

**Conclusion**

In closing, the recession and other economic factors have forced businesses to revisit old business models and implement new ones. Technology and strategies that may have been effective in the past may no longer complement the current landscape. Cloud computing is a business model that enables companies to achieve cost savings and pay-on-demand business solutions. Lastly, shifting non-value-added activities into the cloud provides companies with the ability to focus on their core competencies. Similar to how outsourcing services such as security, facility management and payroll became commonplace, cloud computing solutions can offer similar value.

*The final article of the cloud computing series will explore companies that have been successful in cloud computing and elements that have contributed to their success.*
TH!NK PRIVACY: Locally, globally and across disciplines

By Jennifer L. Saunders

When Barclays Bank PLC won a 2009 HP-IAPP Privacy Innovation Award for its TH!NK PRIVACY program, that was only the beginning.

In just over a year, what began as a cross-company effort to emphasize privacy awareness, compliance and cultural change has expanded into the global, not-for-profit TH!NK PRIVACY Consortium.

From its roots at Barclays, the program has focused on training and awareness as critical components to bring the change that comes when employees understand what they should and should not be doing with personal information, explains Suzanne Rodway, director of privacy, sharestakes and operations/group compliance at Barclays.

The premise behind TH!NK PRIVACY, as included with the coalition's toolkit, states, “Data privacy is an important issue—all organizations have a responsibility to ensure that customer and employee personal data is kept securely and confidentially. Mishandled data can have serious repercussions and can lead to damaged relations, financial penalties and loss of business—reputations are hard won and easily lost. Handling data with care is critical to running a successful business and your employees are your best form of defense.”

Simply put, Rodway says, the TH!NK PRIVACY campaign reminds employees to “press the mental pause button” before taking any action that might endanger personal information.

Barclays' in-house awareness campaign was aimed at changing behaviors and getting people to think about the issues.

The TH!NK PRIVACY logo was created as an eye-catching, message-driven way to reinforce those messages. And, Rodway points out, another key factor was ensuring it could be easily translated into multiple languages and applied across various organizations and businesses that handle private information.

“What we really want them to do is think before they put that unencrypted disk in an envelope or take that unencrypted USB home,” she explains, practices that enable business rather than inhibit it.

Barclay's effort also included a hazard campaign, complete with graphics to illustrate that something as seemingly innocuous as a mobile phone could be a serious danger when used improperly—or inadequately protected. The visuals were posted strategically throughout the building to get people talking about privacy issues.

Posters featuring such images as a cell phone morphing into a grenade and a half-CD, half-buzz saw graphic were used to reinforce the message and eye-catching, memorable ways that “show the double-edged sword with very little wording,” Rodway says. “It was really high-impact.”

Naturally, the next question was whether to share the lessons learned with others, and that sparked a move to get other organizations involved in creating a culture of privacy protection. The project expanded into the TH!NK PRIVACY Consortium, and the UK Information Commissioner’s Office (ICO) responded favorably to the efforts.
Working through a creative agency, Rodway explains, the consortium produced its TH!NK PRIVACY toolkit of materials that can be used by any organization but can be of particular help to those with limited resources for developing their own campaigns.

TH!NK PRIVACY is now an ICO-approved initiative, and its toolkit is available through the ICO Web site.

The result is an open-source approach, Rodway says, with materials that can be tailored to different businesses and nonprofit organizations and can be used across borders and for an array of topics.

The next step? Rodway says the consortium is seeking more members from across the globe and of varied backgrounds and disciplines to continue the creative work of updating the toolkit and sharing best practices on privacy protection.

When it comes to privacy protection, she adds, "If we raise the bar, it helps us all."

More stories by this author:

Privacy law and the challenge of balancing employers' management needs with employee privacy concerns

Understanding the "right to be forgotten" in a digital world

Experts give tips to create and sustain a "culture of privacy"

Privacy law and order: Are there too many cops on the beat?

Experts: ECPA Reform Is Essential

Wi-Fi, Eye-Spy and the unintended consequences of new technology

German Regulator Calls for Termination of U.S. Safe Harbor

Valuing, protecting and commoditizing your personal information: Is "data banking" the answer?
By John Jager, CIPP/C

Regular readers of this column will recall that previously we wrote about amendments to the Alberta Personal Information Protection Act (PIPA) that came into effect May 1, 2010. One of the amendments requires that organizations covered by PIPA notify the province’s privacy commissioner of a loss of, unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a “real risk of significant harm” to an individual.

1. Since this amendment came into effect, the Office of the Information and Privacy Commissioner (OIPC) has published a number of breach notification decisions on its Web site. These published decisions can provide some guidance to organizations that have experienced a breach incident and need to determine if the breach meets the threshold of “real risk of significant harm.”

In Decision P2010-ND-001, an organization was notified that some documents containing personal information had been found in the area of the organization’s U.S. headquarters. The organization recovered a significant number of the documents but was not able to determine whether the files had been disposed of inadvertently as a result of carelessness or if it was an intentional action intended to cause harm.

During the resulting investigation, the organization also discovered that other underwriting files were not in their designated locations and might have been missing from the premises. The OIPC determined that the personal information affected was of moderate to high sensitivity (it included individuals’ names, addresses, Social Security numbers, financial account numbers, drivers' license numbers and more) and could be used to create comprehensive profiles that could be used for identity theft and/or fraud. There was also a real risk due the sensitivity of the information and the fact that the cause of the incident, the whereabouts of the other missing files and the length of time the files had been missing were all unknown.

The OIPC required that the organization notify individuals in Alberta affected by the breach.

As a side issue, it was noted that, although this breach occurred in the United States, the OIPC had jurisdiction, as the personal information involved was that of a number of Albertans and the personal information had been collected by an organization which is licensed to operate in the province.

In Decision P2010-ND-002, the OIPC determined there was a real risk of significant harm after an organization’s payroll files were found in a dumpster. The files had been stored in an offsite locker (the lock had been cut off by an unknown individual), the organization did not keep logs of what records were stored in the locker and it is unknown whether all the records kept in the locker were recovered. Given that the affected personal information included names, addresses, birth dates and SINs, and the fact that cause of the access to the storage locker was unknown, the organization was required to notify former employees (it had already notified current employees).
In Decision P2010-ND-003, a financial organization inadvertently faxed a document containing sensitive financial information to the wrong recipient when transferring a customer's account to another institution. The organization faxed the document to the customer's workplace and a coworker drew attention to the fact that the document was on the fax machine. When the customer notified the organization about the incident, it offered the customer a complimentary subscription to a credit bureau monitoring service. The OIPC determined that although the individual was aware of the incident, the organization had not notified the affected individual and, as there was a real risk of significant harm (it was unknown how long the fax had been left on the machine and there was no way to know how many people may have had access to it), the organization needed to notify the individual.

As can be learned from the above examples, uncertainties about the nature of the event and the fact that the organizations were unaware of how, whom or whether the personal information was accessed contributed to the requirement to notify affected individuals. In each of these cases, the sensitive nature of the personal information disclosed contributed to the decision to require notification. An examination of these cases (there are currently five such decisions on the OIPC Web site) may be of help to organizations in determining whether notification to the commissioner is appropriate under the circumstances.

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.
EUROPE—RFID applications require prior privacy impact assessment

By Jan Dhont & Joanna Tomaszewska

Therefore, the recommendation urges industry to develop an RFID data privacy impact assessment (PIA) framework. RFID operators, i.e. those who determine the purposes and means of a RFID application, including data controllers of personal data using RFID applications, should conduct a PIA and make the results available to the relevant data protection authority (DPA) before its deployment.

The PIA framework should:

- support the principle of “privacy-by-design” by addressing privacy protections embedded in the technology;
- sensitize RFID operators by addressing the technical and organizational safeguards that need to be undertaken to secure personal data from unauthorized access or disclosure;
- enable both operators and DPAs to better understand the privacy and data protection impacts of RFID applications. Knowledge on PIA results is considered useful to DPAs to develop relevant RFID privacy guidelines for companies.

The recommendation requires industry to submit the proposed PIA framework to the Article 29 WP for approval. The Article 29 WP already assessed an earlier proposal for a PIA framework in a different recent opinion (of July 13, 2010, hereinafter: Opinion). Three main elements need to be addressed by the framework since they trigger the Article 29 WP’s concern:

- Identification of the privacy risks associated with the intended use of a specific RFID application
- Assessment of the privacy risks associated with the use and carrying of RFID tags in everyday life
- Clarifications on how RFID tags can be deactivated when used in the retail sector

Given these concerns, the Article 29 WP decided not to endorse the submitted framework proposal and encourages industry to improve the proposal based on the comments expressed in its opinion.

Jan Dhont heads the privacy practice of Lorenz Brussels. He specializes in data protection and privacy, telecommunications, media, and technology law. He can be reached at j.dhont@lorenz-law.com.

Joanna Tomaszewska is an associate in the privacy practice of Lorenz Brussels. She has experience in data protection and privacy, media and advertising, technology law and regulatory matters. She can be reached at j.tomaszewska@lorenz-law.com.
EUROPEAN UNION—Towards a new regulation on data protection in Europe

By José-Luis Piñar

The European Commission (EC) has opened a public consultation period (from November 4, 2010, to January 15, 2011) to obtain views on its ideas for addressing new challenges to personal data protection in order to ensure an effective and comprehensive protection to individuals’ personal data within the EU. The document “Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions informs the consultation.”

After the Lisbon Treaty, and since the EU Charter of Fundamental Rights has become legally binding (Art. 8 recognizes an autonomous right to the protection of personal data), the European Commission is considering proposing new legislation in 2011. The legislation would be “aimed at revising the legal framework for data protection with the objective of strengthening the EU’s stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention, taking into account the specificities of these areas.”

The document begins by stressing that the Directive 95/46/CE “set a milestone in the history of the protection of personal data in the European Union,” and its core principles “are still valid.” But the document immediately notes that “rapid technological developments and globalization have profoundly changed the world around us and have brought new challenges for the protection of personal data.”

Like technology, the document says, “the way our personal data is used and shared in our society is changing all the time.” The challenges posed include addressing the impact of new technologies, enhancing the internal market dimension of data protection, addressing globalization and improving international data transfers, providing a stronger institutional arrangement for the effective enforcement of data protection rules and improving the coherence of the data protection legal framework.

The key objectives of the comprehensive approach on data protection are grouped under five headings. The first one is to strengthen individuals’ rights. In this sense, among others, the following objectives of the European Commission can be highlighted:

- introducing a general principle of transparent processing of personal data in the legal framework
- introducing specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children
- drawing up one or more EU standard forms (“privacy information notices”) to be used by data controllers
- to examine the modalities for the introduction in the general legal framework of a general personal data breach notification
- strengthening the principle of data minimization
- clarifying the so-called “right to be forgotten,” i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes; to make remedies and sanctions more effective.
The second objective is to enhance the internal market dimension. To this end, the EC will:

- examine the means to achieve further harmonization of data protection rules at the EU level
- explore different possibilities for the simplification and harmonization of the current notification system
- examine how to revise and clarify the existing provisions on applicable law, including the current determining criteria, in order to improve legal certainty
- examine some elements to enhance data controllers' responsibilities (making the appointment of an independent data protection officer mandatory, including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, promoting the use of PETs and the possibilities for the concrete implementation of the concept of "Privacy by Design"
- encourage self-regulatory initiatives and explore EU certification schemes.

Third, the commission considers it advisable to revise the data protection rules in the area of police and judicial cooperation in criminal matters. To this end, it will consider the extension of the application of those rules to such areas.

On the other hand, the commission makes reference to the global dimension of data protection. In this context, the commission intends to examine how to improve and streamline the current procedures for international data transfers, including legally binding instruments and “Binding Corporate Rules” in order to ensure a more uniform and coherent EU approach; how to clarify the commission’s adequacy procedure, and how to define core EU data protection elements, which could be used for all types of international agreements.

Also, it will promote universal principles by promoting the development of high legal and technical standards of data protection in third countries and at an international level; striving for the principle of reciprocity of protection in the international actions of the EU; enhancing its cooperation with third countries and international organizations, and following up the development of international technical standards by standardization organizations.

Finally, the document stresses that the implementation and enforcement of data protection principles and rules is a key element in guaranteeing respect for individuals' rights. In this context, the commission will examine how to strengthen, clarify and harmonize the status and the powers of the national data protection authorities, including the full implementation of the concept of complete independence; ways to improve the cooperation and coordination between data protection authorities, and how to ensure a more consistent application of EU data protection rules across the internal market.

In conclusion, it appears that the European Commission is committed to revising the legal framework of data protection in Europe. Always starting from the basis of considering data protection as a fundamental right, that has very significant economic implications whose clarification is essential in the field of international transactions.

Jose-Luis Piñar Mañas, Ph.D. is an attorney at Pia Maaas & Asociados Law Firm, and a professor of administrative law. He also is the former director of the Spanish Agency for Data Protection and former Vice-Chairman of the Article 29 Working Party and Honorific President of the Ibero-American Network of Data Protection. He can be reached at jlpinar@pmasociados.com.
FRANCE—Unlawful implementation of a location-based system sanctioned by court

By Pascale Gelly and Caroline Doulcet

In France, employers who want to monitor employees’ use of company cars using location-based systems must comply with labor and data protection laws. An employer who intended to dismiss an employee for serious misconduct because his vehicle’s location-based system revealed that he used the company car for personal purposes and violated the highway code, has learned this the hard way.

In a ruling of September 14, 2010, the social chamber of the Court of Appeal of Dijon stated that the dismissal of an employee justified by evidence produced by a location-based system in violation of labor and data protection laws was invalid (i.e., not based on a real and serious ground) because it was based on unlawful evidence.

The court considered that the location-based system had not been implemented lawfully because employees had neither been informed of its implementation nor of the personal data processing involved and because the location-based system had not been notified to the CNIL. The employer claimed having provided employees with an internal memo informing them of the use of technical means to ease travels and client assistance. However, this document failed to refer to a “location-based system.”

The employer has been sentenced to pay the employee 8,000 euros in damages, which corresponds to the amount the employee would have been paid by the employer had he not been unduly dismissed for serious misconduct. Moreover, the employer has been sentenced to pay 1,000 euros in damages to the employee for bad faith performance of the employment contract by the unlawful implementation of a location-based system.

Pascale Gelly of the French law firm Cabinet Gelly can be reached at mailto:pg@pascalegelly.com.

Caroline Doulcet is of the French law firm Cabinet Gelly and can be reached at mailto:cd@pascalegelly.com.
FRANCE—Targeted advertising: A charter to protect Internet users

By Pascale Gelly and Caroline Doulcet

A public consultation launched by the Secretary of State for the future and development of the digital economy has revealed that one of individuals’ major concerns about targeted advertising is the fear that their advertising profiles could be kept indefinitely.

The need for a right to be forgotten in the digital era has been the focus of the Secretary of State since November 2009.

Public consultation, debates among professional associations and members of the government on the subject has led to the signing of a charter “on targeted advertising and protection of Internet users” by 10 industry associations under the coordination of the UFMD, one of the major direct marketing associations in France.

The charter contains eight recommendations to protect the privacy of Internet users and minors, among others, in the context of targeted advertising:

- providing Internet users with clear and easily accessible information related to targeted advertising implemented in the Web sites they are consulting (e.g; the techniques used to adapt the content of adverts online, the technical means used, the type of information processed)
- providing Internet users with ways to express their free choice by giving them the chance to accept or refuse the display of targeted advertising
- creating a legal framework for linking behavioral data and personal data—each time an entity wants to link behavioral data and personal data, it should inform Internet users and provide them with the possibility to accept or refuse such use of their data unless it is not legally required (e.g if linking is necessary to perform the services asked by the Internet user). When several entities want to link together their behavioral data and personal data, such processing should be subject to the prior consent of Internet users
- providing individuals with the choice to accept or not to be geo-located via their mobile phone
- taking into account the right to be forgotten in the digital era concerning cookies. The charter stipulates that the period of analysis of cookies used for behaviorally targeted advertising should be proportionate to the buying cycle of the product or service promoted through such advertising. The average duration of a buying cycle has been estimated at about 60 days by default
• ensuring the specific protection needs for private correspondence and for minors. In particular, no behavioral category may be created in relation with the interests of minors under the age of 14. Moreover, adverts targeting minors must comply with professional ethical rules
• implementing “capping” systems in order to limit the number of targeted adverts displayed
• encouraging the use and the development of technical protection devices to protect privacy and personal data and of anonymization systems.

Pascale Gelly of the French law firm Cabinet Gelly can be reached at mailto:pg@pascalegelly.com.

Caroline Doulcet is of the French law firm Cabinet Gelly and can be reached at mailto:cd@pascalegelly.com.
FRANCE—CNIL issues guidelines on data security

By Pascale Gelly and Caroline Doulcet

The use of IT systems has become essential for analyzing and centralizing information and outsourcing is increasing, thus the security of information systems is a major challenge for any data controller, whether a business or government entity.

Taking into account this evolution, in October, 2010, the CNIL issued guidelines related to the security of personal data. There is a questionnaire on CNIL's Web site to help any data controller assess the level of personal data security within its entity.

The guide addresses 17 topics through data security fact sheets. It describes the minimum security measures to be put in place and the mistakes to be avoided. It also provides information on more specific security matters.

The security topics covered in the fact sheets include: risk analysis, user authentication, management of authorizations of use and users sensitization, computer security measures (against fraudulent access/use or virus), security of mobile devices, backups and business continuity, maintenance, management of incidents, security of premises, security of internal network, security of servers and software, outsourcing, archiving, exchange of information with other entities, software development, anonymization and encryption.

The CNIL recommends that data controllers, among others, set up internal rules on the use of information systems by employees.

Pascale Gelly of the French law firm Cabinet Gelly can be reached at mailto:pg@pascalegelly.com.

Caroline Doulcet is of the French law firm Cabinet Gelly and can be reached at mailto:cd@pascalegelly.com.
Commissioner receives OBA Karen Spector Memorial Award for Excellence in Privacy Law

By Jennifer L. Saunders

Canadian Privacy Commissioner Jennifer Stoddart has been honored by the Ontario Bar Association (OBA) with its Karen Spector Memorial Award for Excellence in Privacy Law, which was established to recognize, honor and celebrate the outstanding achievements of OBA members working in the privacy field.

In announcing the selection of Stoddart, who received the prestigious award at a dinner ceremony in Toronto on October 18, the OBA noted, “While there was no shortage of exceptional members of the bar worthy of this award, it was unanimously agreed that the accomplishments of Jennifer Stoddart as Canada’s privacy commissioner made her the obvious choice to be recognized this year.”

Stoddart, who is completing her seven-year term as Canada’s privacy commissioner, was selected for her role in establishing the OPC as a leading regulator on privacy issues, and the OBA praised her work on such issues as youth online privacy, cross-border data protection and coordinated global privacy enforcement. The association also praised Stoddart’s efforts to create a contributions program for not-for-profit organizations and consumer groups to advance privacy and data protection research, policy and education and her leadership in what the OBA described as an “unprecedented collaboration involving 10 data protection authorities on four continents who issued a joint statement regarding the respect of privacy laws by technology companies launching new products.”

OBA Privacy Law Section Chair Laura Davison presented the award to Stoddart at the October event, which was also attended by past recipients Priscilla Platt, Mary O’Donoghue and Jeffrey Kaufman.

In announcing Stoddart as the recipient of the 2010 award, Davison noted that while recipients need meet only one award criteria, Stoddart actually met all five categories of legal contributions to the practice of privacy law; contributions to the development of privacy law through writing or public speaking; organizational contributions; outstanding mentorship, and other exemplary achievements.

“In Commissioner Stoddart’s case, there are many,” Davison said, describing Stoddart as “an outstanding and more-than-worthy recipient of the OBA’s Karen Spector Memorial Award for Excellence in Privacy Law.”
Jonathan Cantor joins Department of Commerce

Jonathan R. Cantor, CIPP, CIPP/G, was recently selected as the chief privacy officer and director of open government at the Department of Commerce. In his new role, Cantor will work with all of the bureaus and operating units to improve the department’s privacy program, develop sound privacy policies and consult with public- and private-sector professionals and organizations.

Cantor came to the Department of Commerce from the Social Security Administration (SSA), where he served as the executive director for privacy and disclosure and led the SSA privacy program.

He also serves as co-chair of the Innovation and Emerging Technology Subcommittee of the CIO Council’s Privacy Committee. He is a graduate of Duke University and received his J.D. from George Washington University.

Hear from Jonathan Cantor on December 9 at the Practical Privacy Series: Government.
Jules Polonetsky, CIPP
Co-chairman and Director
Future of Privacy Forum

In this last interview of our yearlong feature celebrating the IAPP’s tenth anniversary, the Privacy Advisor chats with Future of Privacy Forum co-chairman and director and past IAPP board member Jules Polonetsky about, well, what else? The future of privacy.

Privacy Advisor: What is the future of privacy?

Jules Polonetsky: One of the most exciting paths that could lead to more responsible online practices is the advancement of identity management and trusted identity solutions. Through the years, there have been fits and starts in architectural developments in this area but no major support from most businesses or government—and no real consumer demand. Today, the U.S. government has developed an identity exchange framework for accessing its online services, and on the other end Facebook Connect has been implemented on several hundred thousand Web sites. It seems clear that people are ready to employ ID systems for convenience and personalization. The big question now for companies ranging from banking to marketing is how to build the privacy and business models to give consumers both greater personalization and more control. At a time when reliance on anonymization is becoming harder, and with policymakers and progressive companies looking for solutions to replace the notice-and-choice model, trusted identity management could be the path that allows for both profits and responsible data use.

Privacy Advisor: What privacy-related questions are on your mind these days?

Jules Polonetsky: We are grappling with the gray area that exists between the public and private domains online. We understand what public means, we understand what private means—what’s in the middle causes tension. We may make our information available beyond our friends because we want like-minded users to have access to our information, but we don’t want people to use it in ways we don’t like, we don’t want everyone to access it. Is there a feasible blurry-edged network concept that allows us to be open but also have outer boundaries? Can we support this area of gray, semi-public, but still leaving the user some control over out-of-context uses? And how can technology or law address this effectively in a way that doesn’t adversely impact the benefits to a society of public records and free speech rights?

Another developing issue that will determine the future of privacy is how government and industry handle the development of the smart power grid. Billions are being spent to help better manage power usage and help the environment by turning our power system into a two-way electricity Internet that will share data about device usage at 15-minute intervals. You will realize that running your dishwasher during off peak times will save money and power. Your smart washing machine will alert your fridge not to make ice or defrost while the wash is going through. But this means that information about what room you’re in at what time, how long you watch TV, when you do a wash, that you microwave frozen meals for dinner and how far you traveled in your electric vehicle will be available to third parties. Will we learn lessons from the successes and failures of the Internet? Can this system, which some predict will be larger than the Internet, also respect privacy? Make way for the smart CPOs of the smart grid!
A particularly challenging area, and one where the Future of Privacy Forum has partnered with the Center for Democracy and Technology, is the new world of “apps.” Millions of developers around the world are building great new programs on mobile and social media platforms. Despite limited expertise in privacy or security, these new companies rapidly become the custodians of detailed personal data, often including real-time locations, of millions of users. We can’t delay in helping the app community develop the expertise and best practices needed to succeed.

To read other interviews from the series, click on the links below.

Jennifer Barrett, CIPP, Global Privacy and Public Policy Executive, Acxiom Corporation

Alan Chapell, CIPP, President, Chapell & Associates, LLC

Suzanne Rodway, Group Privacy Director, Barclays Bank

Kathleen Street, CIPP, Privacy Officer, Children’s Health System

Jonathan Fox, CIPP, Global Privacy Director, eBay

John Kropf, CIPP, CIPP/G, Deputy Chief Privacy Officer and Senior Advisor for International Privacy Policy, Department of Homeland Security

Lawrence Tan, CIPP, CIPP/G, Assistant Director, Ministry of Health Holdings, Singapore

Scenes from Privacy After Hours.
See photos