Greetings,

At the IAPP Global Privacy Summit in March, during a session featuring authors Cory Doctorow and Jeff Jarvis, an audience member asked, “Is privacy dead?” No, answered Jeff Jarvis, “privacy has more protectors than ever before in privacy history.”

This certainly rings true. The IAPP passed the 10,000-member milestone last month, and since then, hundreds of new members have joined. These new members come from increasingly varied industry and economic areas—after all, data is everywhere.

In this edition of The Privacy Advisor, we kick off a series to explore some of data protection’s newest roles. They are increasingly diverse, and this diversity could be a great boon to our profession. The efficacy of a multidisciplinary approach toward problem-solving is well known. Having a multitude of perspectives on data privacy offers promise.

I am delighted to introduce you to Lina Ornelas in this issue. Many of you know Lina from your work with IFAI—the Instituto Federal de Acceso a la Información y Protección de Datos—Mexico’s federal data protection authority. Lina is IFAI’s general director for privacy self-regulation. Yes, that is a unique position within our field. As you will read, Lina is working with the Ministry of Economy in Mexico to create a self-regulatory framework for data controllers.

Self-regulation is high on the minds of data protection regulators and industry players alike these days, and the U.S. Federal Trade Commission just gave the topic a shot in the arm on the release of its long-awaited privacy report, which urges industry to put the pedal to the metal on self-regulatory efforts.

Can self-regulation work in the data protection and privacy sphere? Let us know what you think.

Sincerely,

J. Trevor Hughes, CIPP
President & CEO, IAPP
Rewind 11 years. If you worked on data privacy matters, you were probably a law firm partner, a consultant, privacy officer or one of a handful of people bearing the title “chief privacy officer.”

In 2001, privacy and data protection professionals were barely a speck on the tech economy's radar.

Time has marched on, and the digital revolution has steamrolled a great swath to new avocations—from digital reputation management to privacy engineering—in addition to carving out new roles in advocacy, policy, academia, publishing, recruiting and a multitude of other areas that have turned their focus to data privacy over the past decade.

Enter privacy’s next phase.

The IAPP has witnessed every moment of the field’s evolution from a close-knit clutch of compatriots to the burgeoning multinational community it is today.

“Privacy has never been a singular profession,” says Trevor Hughes, CIPP/US, president and CEO of the IAPP. “Historically we have had tremendous diversity in the background and the day-to-day workings of privacy pros. Today, that diversity is exploding.”

Introducing your new colleagues and peers

Starting with this issue of The Privacy Advisor, the IAPP is kicking off a series to showcase these new roles. They are less traditionally associated with data privacy, but they are very much part of the future of privacy.

The new privacy professionals are presidents and CEOs, senior product managers, CISOs, sales executives, human resources associates, marketing managers, town clerks, national data protection officers, IT managers, webmasters, data architects, security architects and a great many other roles that touch data in some way.

Like Angie Anderson, a human relations privacy manager who conducts privacy training, administers policy development and handles other facets of employee and employment-candidate privacy. Despite the HR title, Anderson says she spends about 90 percent of her time on data privacy matters.

Others spend only a portion of their time on privacy. Kimberly Atherton, a marketing data steward at IBM, directs about 60 percent toward privacy, working with the legal department and privacy office to upkeep privacy guidelines and educate fellow employees.

“My job requires that I communicate and educate about data privacy either one-to-one, with small groups or through more broad education programs,” Atherton says, adding that even though she’s not 100-percent privacy focused, she considers herself a privacy professional.

Victor Clark, CIPP/US, is data privacy’s equivalent to the Major League closer; he spends only a little bit of time in the game, but his role is instrumental.

Clark is operations director at FirstData. He self-identifies as a privacy professional who spends about 25 percent of his time on privacy and the remainder on “customer service, the voice of the customer,”
business process improvements, performance improvements, process management controls, litigation avoidance quality assurance, training and compliance audits.” Clark implemented the privacy program at FirstData’s consumer reporting agency, where he established privacy as a shared priority across all of the company’s business areas. Business area administrators (BAAs) are responsible for making privacy happen.

“Each BAA represents their organization at privacy meetings and assists in developing a privacy/confidentiality culture within their organization,” Clark explained to The Privacy Advisor.

Anderson, Atherton and Clark are just a few of the new types of privacy professionals the IAPP is seeing more of. Their roles exemplify information privacy’s spread across an increasing array of sectors and into mainstream society. In the coming weeks and months, we’ll introduce you to many others.

Help us shape it
The Privacy Advisor is excited to kick off this series about members, and we would like to hear from you. Tell us about your work in the profession and how you became involved in data protection and privacy. (We will seek permission before publishing submissions.)

—IAPP Staff
Czech Constitutional Court takes on data retention rules

By Vojtech Chloupek

In less than a year, the Constitutional Court of the Czech Republic issued two decisions that repealed most of the data retention legislation.

By its first judgment from 22 March 2011, the court repealed the obligation of telecoms operators and ISPs to retain traffic and location data for the minimum period of six months and maximum period of 12 months and to provide such data to authorised bodies upon request (First Judgment).

Already in its decision, the court mentioned also Section 88a of the Czech Criminal Procedure Act, No. 141/1961 Coll., which entitles investigative and prosecuting bodies to obtain data from providers of electronic communications services which are otherwise subject to a telecommunication secret or where data protection applies. This provision, being directly linked to the repealed provisions relating to telco operators and ISPs, was also problematic according to the Constitutional Court. However, as the constitutional complaint did not address the Criminal Procedure Act, the court could not decide about Section 88a. It was therefore for someone else to pick up the hint, and it did not actually last long. The District Court of Prague 6 filed a constitutional complaint challenging Section 88a on 1 July 2011, and the Constitutional Court issued its decision on 20 December 2011 (Second Judgment).

In the reasoning of its motion, the District Court contrasted the general restrictiveness of requirements for ordering wiretapping and recording of the telecommunication operation to extensive indulgency of requirements for ordering the detection of data about telecommunication operations as laid down by Section 88a, the Repealed Section. The District Court especially argued that such indulgency inevitably leads to inflation of motions to order the detection made by the police, the customs as well as the military police, thus undermining the court’s position as a guardian of constitutional rights guaranteed in the criminal proceedings. Not surprisingly, the District Court predominantly referred to the aforementioned First Judgment.

In the First Judgment, having repealed Section 97 (3) and (4) of the Act No. 127/2005 Coll., the Telecommunications Act, on basis of which the collection of telecommunication data by operators and providers of Internet connection was possible, the Constitutional Court said that from the collected data it could be, with 90-percent accuracy, deduced how often and who the user met, who were the user’s friends or colleagues and what the user’s activities were. The Constitutional Court ruled that such a global collection of personal data constituted a breach of the rule of law and invaded the privacy of each phone or Internet user.

Having invoked the factual coherence, in the Second Judgment the Constitutional Court also reiterated to great extent its argumentation from the First Judgment. As it is repeatedly mentioned in the Constitutional Court’s case law, despite not being explicitly mentioned in the Charter of Fundamental Rights and Freedoms which forms part of the Czech constitutional order, the confidentiality of communications shall encompass not only the content of messages as such but also other data detected
during the telecommunication operation concerning one's person, since the dynamically evolving right to privacy needs to be apprehended in its time context, especially with respect to the development of technical and technological possibilities which inevitably increase the state's potential to interfere with the rights and liberties of its citizens.

In reference to the German Federal Constitutional Court's judgment from 15 December 1953 (Volkszählungsurteil) and to the case law of the European Court of Human Rights, the Constitutional Court primarily emphasised everyone's fundamental right for the informational self-determination as a facet of the right to privacy: "In other words, the right to privacy also guarantees the right of an individual to decide at one's own discretion if and to which extent, in what ways and under which circumstances should personal data and information be disclosed to other entities."

Subsequently, using the test of proportionality, the Constitutional Court scrutinised the Repealed Section from the viewpoint of the constitutionality of its interference with the fundamental right to informational self-determination. Although the Repealed Provision was found to effectively pursue a legitimate objective consisting in the protection of public interest in the prosecution of crimes and the prevention of criminality and, moreover, to comply with the EU Data Retention Directive 2006/24/EC, and therefore passed the first step of the test of proportionality, it failed its second step.

The second step consists of assessing whether the detection of data concerning telecommunication operations by authorised bodies is subject to the requirement of necessity. Under the Repealed Section, the only condition for the ordering of detection of data on a telecommunication operation was that such a measure should lead to "clarification of facts important for criminal proceedings." In view of the Constitutional Court this was excessively broad, enabling authorised bodies to request data literally whenever any connection with the criminal proceedings occurred. In that context, it was pointed out that the respective authorities overused this and requested even data concerning petty crimes. The Constitutional Court also made the point that, taking into consideration the intensity of the interference with the right to privacy, such a measure cannot be understood as a usual or routine means of crime prevention. Simultaneously, the Constitutional Court criticised the absence of legal rules for securing the collected data and the absence of a legal obligation to subsequently inform the data subjects about the collection and retention of the data.

For the purposes of completeness, the Constitutional Court added that the Repealed Section would have also failed the last, third step of the test scrutinising the proportionality in the strict sense since it did not assign any importance to the nature and seriousness of the crime for which the criminal proceedings had been conducted.

On 27 February, in response to both the First and the Second Judgment, the Czech Government proposed a bill to replace the repealed provisions. As it is explained in the reasoning report to the proposal, the importance of traffic and location data which can reveal who, from where, with whom and how long communicated, lies in the fact that such data can be cardinal in order to detect a perpetrator of a crime. Traffic and location data may also serve to find missing persons, such as minors, seniors suffering from dementia or suicides. The proposal came into existence as a result of a struggle that the government underwent in order to present a draft of legislation which would enable the retention of traffic and location data in such a way that requirements posed both by the Directive and the Constitutional Court would be accommodated.
The proposal, which is likely to be passed, should finally bring a solution to the most problematic points of the preceding legal regulation: the body authorised to request traffic and location data are to be enumerated in a strictly exhaustive way; traffic and location data are to be retained for a period of six months from the date of the communication, which is the shortest period required by the Directive, and, in the end, traffic and location data can be requested by authorised bodies only for purposes of criminal proceedings conducted either for a defined serious willful crime or a specifically listed crime. It is going to be interesting to observe if the proposal will effectively reduce the number of requests for traffic and location data by the authorised bodies.

Vojtech Chloupek is senior European counsel in the Prague office of Bird & Bird with broad expertise in intellectual property and information technology. He can be reached at Vojtech.Chloupek@twobirds.com.
APEC’s cross-border privacy rules to facilitate data flows...soon

By Angelique Carson, CIPP/US

The Asia-Pacific Economic Cooperation’s Cross-Border Privacy Rules (CBPRs)—endorsed by U.S. President Barack Obama and APEC member economies at an APEC leaders meeting in Hawaii late last year and scheduled to be released later this year—aim to provide a framework to facilitate cross-border data flows by allowing for interoperability through various jurisdictions’ privacy regimes. The framework is voluntary and essentially self-regulated, though to-be-established enforcement authorities will act as the system’s backbone.

The framework is “very much aimed to provide consumers with assurances that when their data is transferred across borders, that those organizations have received an APEC-approved seal that is aimed to provide them with assurances of trust that there is a baseline of privacy protection that is respected,” said APEC Data Privacy Subgroup (DPS) Chair Danièle Chatelois. “You’ve got choice; you’ve got notice; you’ve got access rights, security safeguards. In order to be recognized under the APEC seal, those privacy protections have to be in place.”

The DPS recently gathered in Russia for a meeting its members describe as having been especially productive with the accomplishment of three tasks crucial to the rules’ implementation.

First, the DPS endorsed the document that member economies will use to apply to the system, assuming the economy can demonstrate that its data privacy standards meet baseline requirements on principles such as consent, notice, choice and security.

Second, the DPS endorsed a package of documents that would establish “accountability agents,” private-sector, third-party verifiers tasked with determining the validity of applicants’ privacy regimes and making recommendations on whether the applicant should be accepted into the framework. The CBPRs’ dependence on accountability agents may help to alleviate a common problem plaguing enforcement authorities globally: limited resources. In the case of binding corporate rules (BCRs), for example, companies must work through data protection authorities (DPAs) for assessments and approvals, an expensive and timely process.

New Zealand Assistant Privacy Commissioner Blair Stewart believes that accountability agents will be significant in that they will take some of the strain off of public regulators, noting, “It hasn’t gone operational yet, so it has to be tested. But if it does work, it seems to me it can scale up...based on private-sector flexibility...Public bodies are never going to be able to scale up so successfully given how public bodies are funded. I think it’s a really valuable, useful feature of the APEC system...I think it has a great deal of promise.”

The agents will reassess member companies’ privacy regimes and policies periodically to be sure compliance with CBPRs is maintained year after year—especially as business needs and market forces shift. A built-in dispute resolution mechanism establishes DPAs as “backstop authorities” in cases of noncompliance with CBPR provisions.
To become an accountability agent, an entity must apply to a "joint oversight board" in order to be recognized as such. The board—the DPS's third tangible success in Moscow—is not only to establish accountability agents but also to suspend agents should a violation occur.

The board is comprised of three member economy representatives and will be responsible—perhaps more importantly at this early stage—for accepting and reviewing member economies’ applications and making recommendations on whether the applicants should be accepted. APEC leaders will then vote based on those recommendations.

Josh Harris, who will chair the Joint Oversight Board for a two-year term, said the impetus for CBPRs is twofold.

"The first is consumer confidence. We want to make sure consumers have a mechanism to understand who they are doing business with and understand what privacy practices and policies a company has in place. That's really important to continuing the growth of the digital economy," he said. "The second is to promote interoperability."

In creating safety provisions to promote consumer confidence in e-commerce, it's important that thought leaders and regulators take caution not to "inadvertently build up unnecessary barriers against the free flow of information across international borders," Harris said.

The focus on cross-border interoperability—rather than harmonization—helps resolve a tension persistent in other global frameworks, Stewart noted.

Frameworks aiming to harmonize fail to recognize that “everyone in the world does things differently” and struggle when they aim to achieve goals by asking myriad parties to meet the same standards in exactly the same way, Stewart said. This is especially problematic across economic brackets.

"At the end of the day, when you are looking globally, you'll never be able to harmonize," he said. "So probably the interoperability philosophy, at a global level, is more feasible at the moment."

The system, which aims to eventually see every APEC member economy sign on, recognizes that local privacy requirements will still exist. It does not aim to negate those rules, noted Markus Heyder, counsel for international consumer protection at the U.S. Federal Trade Commission (FTC).

"Companies are always responsible for local privacy requirements that may or may not be different," Heyder said, “but overall, we think this will streamline data flows and make privacy protection more efficient for companies...and will therefore have better results for consumers.”

Looking forward, the DoC’s Harris says the DPS is working on a number of bilateral initiatives and is speaking with representatives from government and industry globally. It recently met with the French data protection authority to discuss how similarities between Europe’s BCRs and APEC’s CBPRs could potentially be leveraged. In addition, the DPS has been looking at a potential joint project between the U.S. and China, examining the ways in which a CBPR certification may help Chinese tea manufacturers to reach a more international base.

Heyder says companies should feel incentivized to enroll in the program not only because it promotes e-commerce and international data flows but because, from the FTC's perspective as an enforcer,
participants that can demonstrate they’ve worked toward compliance would likely have an easier time when it comes to enforcement decisions.

“There’s a stronger recognition now that companies need to be able to show regulators that they are trying to comply with the appropriate privacy protections, either under applicable laws or self-regulatory programs,” Heyder said. “While it’s not a safe harbor from law enforcement, it’s definitely a factor in making law enforcement decisions and where to deploy a law enforcement resource.”

At the 2012 IAPP Privacy Summit in Washington, DC, FTC Commissioner Edith Ramirez, Hewlett-Packard’s Scott Taylor, CIPP/US, and TRUSTe’s John Tomaszewski discussed the rules’ ongoing development. Indeed, Taylor said, the CBPR system gives his company some comfort in its ability to move data throughout very divergent countries.

“Very quickly, it’s doing things to help organizations partner together or organizations providing services and handling data to be recognized by other companies and uphold some level of standard,” he said.

Chatelais says she’s very confident in the practical application of CBPRs in the near future.

“The system we’re developing is aimed to achieve concrete results,” she said. While APEC “does not necessarily work in the abstract policy realm... The objective of this is very much geared to implementing it and rolling it out and adopting it and having member economies participate.”
IRS taxpayer authentication program combats identity theft: A Q&A with Rebecca Chiaramida

As more Americans file their taxes online, protecting highly sensitive financial data from identity thieves is a major concern for taxpayers and the Internal Revenue Service (IRS) alike. The Privacy Advisor recently caught up with IRS Director of Privacy, Government Liaison and Disclosure Rebecca Chiaramida, CIPP/G, to explore a new authentication program recently initiated by the agency to combat a rise in refund fraud schemes and identity theft.

The Privacy Advisor: How common is identity theft with regard to federal tax returns? Is tax identity theft on the rise?

Chiaramida: Over the past few years, the IRS has seen an increase in refund fraud schemes in general and those involving identity thefts in particular. Identity theft and the harm that it inflicts on innocent taxpayers is a problem that we take very seriously. In 2011, our Identity Protection Office stopped more than 260,000 fraudulent returns and protected more than $1.4 billion in refunds. We understand that this is a frustrating situation for victims. Identity theft protection is a top priority for the IRS, and we’re taking concrete steps to not only assist taxpayers who have become victims but prevent it before it occurs. It’s important to note that although identity thieves steal the information from sources outside the tax system, the IRS is sometimes the first to inform the individual that identity theft has occurred.

The Privacy Advisor: Have there been any coordinated efforts with tax preparers to help prevent ID theft?

Chiaramida: Most professional tax return preparers and the organizations they work for have a strong set of ethics and share our commitment to taxpayers to help them prevent identity theft. So yes, it’s a partnership.

The IRS continues to conduct outreach to provide taxpayers, return preparers and other stakeholders with the information they need to prevent tax-related identity theft and when identity theft does occur, to resolve issues as quickly and efficiently as possible. For example, in preparation for the 2012 filing season, we worked closely with software developers on inclusion of the Identity Protection Personal Identification Number, or IP PIN. We’ve also done a great deal of targeted outreach to educate return preparers on the IP PIN’s use. Additionally, we recently launched a section on IRS.gov dedicated to identity theft matters, including tips for taxpayers and a special guide to assistance ranging from contacting the IRS Identity Protection Specialized Unit to tips to protect against “phishing” schemes.

The Privacy Advisor: How did you come up with this new program? Was it influenced by a preexisting model? Were there other authentication methods under consideration that ended up not being used?

Chiaramida: The supplementary verification process known as the Identity Protection Personal Identification Number, or IP PIN, expands on last year’s pilot program and is geared to protect victims with previously confirmed cases of identity theft.

The IP PIN was developed to protect revenue, reduce burden on identity theft victims and increase operational efficiency. The purpose of the IP PIN was to provide an efficient method for processing tax
returns that are marked with an identity theft indicator while still protecting the taxpayer’s personal information.

There was no preexisting model at the IRS but a clear need for additional security. A taxpayer authenticates directly to the IRS by submitting documentation that validates the legitimate owner of the SSN. The IP PIN initiative will create an additional layer of security on these accounts. It is another tool at our disposal to protect identity theft victims and revenue.

**The Privacy Advisor: What other factors went into drafting this program?**

**Chiaramida:** To accommodate the IP PIN program, we revised the 1040 series tax forms to allow for IP PIN entry; met with software developers to ensure their programming accommodated the IP PIN, and developed a communication and outreach strategy for taxpayers, tax preparers and key stakeholders.

**The Privacy Advisor: What happens if an ID thief accesses a taxpayer’s IP PIN number? Are there additional layers of authentication available for a taxpayer?**

**Chiaramida:** Like any other sensitive or personal information, there is always a possibility that the IP PIN may be compromised, but we are taking steps to minimize that risk. The purpose of the IP PIN is to validate the identity of a taxpayer during the filing of the current year tax return. We implemented specific authentication processes for those taxpayers who were issued the IP PIN to minimize the possibility of harm if the IP PIN is compromised. Taxpayers will receive a new IP PIN each December for use in filing their current year tax return.

**The Privacy Advisor: How many resources—employees, systems, etc.—are going into this new program?**

**Chiaramida:** We have substantially increased our resources devoted to both prevention and assistance. Even in a declining budget environment, we are hiring and training new staff to address the growing challenge of identity theft.

The IRS is committed to continuing to improve our programs. We will work to prevent the issuance of fraudulent refunds and work with innocent taxpayers to clear their accounts and get them their money in a courteous and professional manner. The IRS has taken actions to be better prepared in both fraud prevention and victim assistance.

On the prevention side, this means implementing new processes for handling returns, new filters to detect fraud, new initiatives to partner with stakeholders and a continued commitment to investigate the criminals who perpetrate these crimes.

As for victim assistance, the IRS is working to speed up case resolution, provide more training for our employees who assist victims of identity theft and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly. These improvements would not be possible without the additional resources that have been directed toward these programs.

**The Privacy Advisor: Will this program be expanded or changed based on this year’s results?**

**Chiaramida:** This year’s initiative is an expansion of last year’s pilot program of the IP PIN. It is one tool in our arsenal as we take a comprehensive approach to stopping identity theft and refund fraud. The IRS will analyze the results of this year’s IP PIN program to make any necessary enhancements to the program and determine potential expansion for the 2013 filing season.
The Privacy Advisor: *Is there anything you would like to add/discuss that we have not touched upon?*

**Chiaramida:** We understand that resolving the problems associated with identity theft is frustrating for victims, and the IRS is working to resolve cases in which tax records have been affected by identity theft as quickly as possible and have committed significant resources to this effort. The identity theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain. The IRS is firmly committed to working with taxpayers to take care of these problems as quickly as possible.
Getting to know a privacy pro

Lina Ornelas, general director for privacy self-regulation at Mexico’s Instituto Federal de Acceso a la Información Pública, talks laws, goals and self-regulation

By Angelique Carson, CIPP/US

On July 5, 2010, the Mexican Federal Law on Protection of Personal Data Held by Private Parties was officially published. This legislation establishes minimum standards that people who use others’ personal data are obliged to comply in order to protect privacy. Additionally, in order to detail the law, its Secondary Regulation was issued in December 2011. With this, the legal framework for data protection in Mexico was officially enacted. This achievement signifies a change of paradigm in the Mexican society, as for now, personal information is owned by the data subject and no longer by the person who has it or uses it.

Lina Ornelas is the general director for privacy self-regulation at Mexico’s Federal Institute for Access to Information and Data Protection (IFAI). Ornelas works to understand the way private parties who process personal data think and act to find their incentives to protect personal data, she says. She also works to give such parties tools to enable compliance with the law and promote responsible data processing.

Ornelas is in charge of developing tools to facilitate regulated entities’ compliance with the law, helping them to create privacy notices, for example, through a privacy notice generator available mainly to SME’s. Her office has published recommendations such as data controller designation and is working to develop model contracts for regulated entities to follow. She says that self-regulatory mechanisms will allow data controllers to voluntarily establish and follow additional measures from those already provided by the law. “We have the mission to change the perspective in which these parties see and handle personal information,” Ornelas says.

Working with the Ministry of Economy in Mexico, Ornelas’ team will now work to create a self-regulatory framework which will include a privacy certification system.

The Privacy Advisor caught up with Ornelas to learn a bit more about her work as director for privacy self-regulation and the ways that Mexico’s new law may or may not be changing Mexico’s landscape when it comes to data protection.

The Privacy Advisor: What was your path to privacy?

Ornelas: In 2002, I was working as the General Director of Legislative Studies at the State Department, where I had the opportunity to participate in the group that drafted the initiative the Access to Information Act. In this law, we included a data protection chapter that established principles for the executive branch and also for other branches. A year after, I came to work in the IFAI as Directorate of Classified Information and Personal Data. This was very important considering one of the reasons to classify information is personal data because it is considered confidential, and you need the consent of the data subject to disclose said information to third parties. In 2004, I collaborated in the issuance of some guidelines for privacy, which were published in 2005. That was when we at IFAI noticed that we didn’t have data protection as a fundamental right, and we started working along with a group that
promoted a constitutional reform. On the other hand, it took us nine years to have a law, but fortunately, being late does not necessarily mean less, principally because we had the opportunity to see how the European law was formed, and at the same time I was working in APEC in different groups that gave me the chance to attend to several interesting discussions which were very useful as I took little pieces of different models in order to help in the creation of the Data Protection Law. Our law is considered nowadays a hybrid of the European, U.S. and Canadian models. At the end, it was decided that the IFAI would be the authority, not only for the public sector, but also to the private sector. In 2006, I became a member of the IAPP and I had the opportunity to represent the IFAI in different kinds of meetings, which also gave me valuable insights in this arena.

**The Privacy Advisor:** You hold a rather unique position within the commission in that you are specifically designated to promote self-regulation. What does your role entail?

**Ornelas:** It is indeed a unique position that needs to be very creative and careful as well. Our law has an article promoting self-regulation mechanisms, and it says clearly they have to go above the law to be considered as such. Normally, self-regulation sounds very weak, but our law has a different perspective as it changes completely the way a lot of different sectors see this type of regulation. In Mexico, accountability is a very new thing. For us, companies can decide voluntarily to adopt a self-regulation mechanism, but once they are in, they must comply with several duties and if not, a consequence must take place. To detail these aspects, our law provides that IFAI, jointly with the Ministry of Economy, will elaborate specific guidelines.

I also think self-regulation is a cornerstone of the whole international system. We have a good law in Mexico, and it is well-recognized as the first law that complies with the Madrid Standards of 2009, but there is little to do in cases where the database is not in our territory. Self-regulation could also be a response even if the personal data is not in Mexico.

Likewise, other benefits of self-regulation are that it implies a competitive advantage before consumers and that effective self-regulation mechanisms could be taken into account by the IFAI in order to low fines in case of a law breach occurs.

**The Privacy Advisor:** Many regulators are skeptical about the success of self-regulation so far? Is it a viable model?

**Ornelas:** We are aware that, for some people, self-regulation has a negative connotation that concentrates primarily on avoiding state regulations. But there are other ways to look at self-regulation. For us, as I said before, these mechanisms can be used wisely by enterprises or organizations seeking to attract more consumers by adopting best privacy practices.

A framework regarding third-party privacy certifiers will establish the characteristics and functions the actors must satisfy as well as the conditions in order to grant or revoke privacy certifications. We have to be very careful in this. It has to be well-supervised. There are always people that are going to make profit from this, but what we want is something deeper. What I want to see is that IFAI can have different arms in different organizations working as if they were one authority.

Companies are very interested in self-regulation. In fact, every week we receive notice from a different group interested in preparing their code of conduct. Our main challenge is with small and medium enterprises because they do not even know the law exists. We have to create the culture first, and then let them know that they will receive requests from data subjects which they have to be ready to respond and also have security measures to comply with the law as a whole.

**The Privacy Advisor:** Has the landscape shifted since Mexico’s data protection law passed?
**Ornelas:** People are more or less aware that there is something going wrong because they receive a lot of phone calls or they do not feel very secure; they gave their data to a company, and it is now in the hands of another company. They know that, but they do not realize they have a fundamental right and do not even realize there is a law. But I think it has changed a lot. The European Union is looking at giving us adequacy. And, for instance, the media has started publishing cases of situations where they considered something is not proportionate, like a bus company that takes pictures of passengers when they take the bus and does not ask for their consent. We are receiving a lot of questions from people and a lot of sectors are aware. It is a good starting point. But the weakest part of the chain is the data subject, because I do not think they are aware. They know “my private life is important,” but they do not know they have a mechanism to complain.

What the IFAI is trying to create, in the mind of data subjects as in the data controller’s mind, is, in one word: awareness. If the IFAI focus goes to teaching people the value of their data, our work is halfway done.

**The Privacy Advisor:** *If you had to sum up what “privacy” means to the average Mexican citizen, what would you say?*

**Ornelas:** In general, we can hardly say that there is an “average Mexican citizen;” the problem is that there is not an average Mexican as there is not an average Chilean or Canadian either. We can say that the privacy issues are a concern, mostly, in the metropolitan areas, which are the most developed areas of the country. This represents to us one of the biggest challenges that the IFAI has to overcome. We have to permeate the privacy concerns to all the layers of society and reach all of the corners of the country to build consensual vision in personal data protection matters.

**The Privacy Advisor:** *What do you want to see in the next year or so in terms of progress?*

**Ornelas:** What I want to do is to raise awareness in people so they can push industry towards complying. I would like to see someone say, “I don’t see a privacy notice at this company, so I will change to another one.” I would like to see people making decisions by themselves from the data protection perspective. And especially with children; I have been working on data protection in social networking for industry and for parents in how we can give tools to children in a broader sense to take care of what information they give, because they are not aware sometimes that this information can be used for different purposes or even misused.

When your car is stolen or your bag or something, you notice. But when your data is stolen you do not even perceive it. So the biggest challenge in this area is to raise awareness, and we are focused in that direction.
Location-based services: Why Privacy "Dos and Don'ts" Matter

By Alysa Zeltzer Hutnik

2012 is certain to reflect U.S. consumers' continued love affair with sophisticated smartphones and mobile tablets. For many consumers, one of the driving forces in the popularity of these devices is their ability to run software and mobile applications (mobile apps) using wireless location-based services (LBS). With LBS-enabled services, individuals can share real-time and historical location information online--whether to facilitate a social interaction or event, play games, house-hunt or engage in many other activities. Among other benefits, these mobile services also can quickly enable consumers to locate proximate stores and restaurants, share their current location by "checking" themselves in at venues and navigate to a desired location.

But alongside the benefits, mobile LBS capabilities also involve consumer privacy risks. For example, the top perceived consumer risk of LBS-enabled services is the unintended revelation of a user's home address, and websites like "Please Rob Me" demonstrate the danger of location-sharing by providing a database of empty homes based on users' "check-ins" elsewhere. While these may be some of the more extreme examples, it is not uncommon for some LBS-enabled popular services to omit clear disclosures about the extent to which personal information is collected from the consumer and how it is used, and have a process that obtains informed consumer consent for such data collection. These are not "low risk" academic concerns but rather reflect practices that stand a good chance of inviting the scrutiny of federal regulators, including the Federal Trade Commission (FTC), as well as lawsuits by privacy litigants.

For businesses with an LBS-enabled service that want to avoid being a future legal target, it makes sense to take stock of existing business practices and to identify where updates may be appropriate in light of emerging legal "do's and don'ts." This article describes the rapid growth of the LBS-enabled mobile services market and associated privacy implications, and outlines practical guidance for entities that utilize LBS in their marketing practices.

Overview of the LBS market

LBS technology has become a mainstay in numerous products and services--from Facebook Places, which allows users to check themselves and their friends in at locations such as restaurants and bars, to Foursquare, a location-based social networking website that allows registered users to post their location at a venue and connect with friends. LBS applications can also be linked to existing social media platforms, allowing third-party developers to integrate LBS into their service. For example, The North Face and Sonic are leveraging location-tracking capabilities with ShopAlert, a service that will enhance a customer's shopping experience by providing a personal marketing message to a consumer entering or exiting the retail location. Other websites, like Groupon and Living Social, are testing real-time local offers to users. The concept behind these marketing initiatives is to anticipate what users want based on location information trends.

The market possibilities for LBS are nearly unfathomable. LBS services are expected to generate $10 billion in revenue by 2016, with nearly half from LBS search advertising. Consumers are cautiously optimistic. A large percentage of consumers express discomfort with the concept of advertiser tracking--nearly three-quarters in one study--with a large majority preferring to have the ability to make a choice--whether opt in or opt out--of targeted mobile ads. Yet, a large percentage of consumers surveyed--52 percent--also expressed a willingness to let their usage patterns and personal information be tracked by
advertisers if this resulted in lower product costs or free online content, and 43 percent of consumers said they were willing to receive targeted advertising in exchange for lower fees or service.

So the key question facing many LBS providers is how to strike the appropriate balance in meeting consumer demand in the provision of desired LBS-enabled services without overstepping privacy boundaries.

Do many existing LBS providers fall short on meeting consumer and legal expectations?

In February 2010, the Carnegie Mellon University studied the privacy controls of 89 popular LBS applications. Of those surveyed, only 66 percent had some form of privacy policy. The majority of those with privacy policies collected and saved all data; e.g., location, personal user profile information, and identifying web information such as IP address, for an indefinite amount of time. While 76 percent had some form of privacy controls, the majority of those controls were not easily accessible from the application's main page and were reached only after clicking through multiple screens.

In December, the reputable privacy certification organization, TRUSTe, reported that, of the top 100 U.S. websites, 97 percent had some form of privacy policy in place, though many companies had a "weak understanding" of their privacy policies and the third-party software used on their website. Notably, many companies reportedly did not understand the extent to which they collected personal data from consumers.

These figures at a minimum suggest that there is room for improvement on the privacy LBS front that would better meet consumers' expectations, as well as promote trust and confidence in businesses' privacy practices.

LBS privacy “Do's and Don'ts”

In addition to promoting consumer confidence and trust, adhering to emerging LBS best practices in privacy is likely to reduce the chance of facing an investigation by federal and state regulators, as well as lawsuits by private litigants. For example, the FTC, charged with consumer protection enforcement, has obtained 20-year settlements with numerous companies for engaging in deceptive or unfair practices by collecting personal information from consumers without appropriate disclosures and consent to such practices—including when personal information collection is set as a default—or for engaging in practices that differ from a business's privacy representations. The continued flurry of class-action lawsuits and media scrutiny regarding these types of practices also serve as a warning.

The bottom line: Even in the absence of black-letter law on LBS practices, there are some clear "dos and don'ts" that are worth considering when engaging in business practices involving LBS-enabled services.

A) Privacy on the back end: Due diligence in designing the LBS service

At a minimum, businesses should know what their LBS service does, what type of data it collects and whether that data is shared with affiliates, partners or third parties. Claiming ignorance as to the data flow of consumer location information is not likely to protect a business from privacy-related liability. Accordingly, consider carefully the intentional and unintentional data flows from LBS offerings. Is the data personally identifiable, either individually or when combined with other elements in the company's database? Will it be shared with an online advertiser or marketer or a social media platform like Facebook? Is there a legitimate business reason for the collection, disclosure and retention of such information? Understanding the data flows is the first step in protecting against a LBS privacy mishap.
In performing such due diligence, businesses also should appoint privacy-trained personnel to lead these efforts to ensure that privacy considerations are identified appropriately and satisfied, both at the outset of the design of a new service or product, as well as at periodic intervals after the service or product is released publicly. These are the core principles of the FTC’s "privacy by design" guidance.

B) Privacy on the front end: Be transparent with users about LBS

Treat LBS information collection and disclosure as sensitive personal information, which means being transparent and careful with the data. This includes providing clear disclosures to consumers--before they download the LBS-enabled service--that explain what personal information will be collected, retained and shared; the consumers' choices as to such data collection, and how to exercise such choices; provide a periodic reminder to consumers when their location information is being shared, and if location information previously collected will be used for a new purpose, provide an updated disclosure to the consumer about the new use and an opportunity to exercise their choice as to that new use.

These disclosures should be presented prominently in plain language; i.e., not legalese or technical jargon.

C) Consent

While there can be some flexibility in how a business obtains a consumer's consent to the collection of LBS information, businesses generally bear the burden of demonstrating that they have obtained informed consent to the use or disclosure of location information before initiating an LBS service. Thus, it is not advisable to use pre-checked boxes or other default options that automatically opt users in to location information collection, or any other manner that ultimately leaves the consumer unaware of such data collection. The key is to clearly provide a disclosure about the location information collection, to clearly obtain consumers' consent to use their location information, and to keep accessible, organized business records of such disclosure and consent. It also is advisable to allow consumers to have the option of revoking consent previously given. (As additional guidance, the Center for Democracy and Technology, a consumer and technology advocacy organization, suggests an opt-out/opt-in choice framework: LBS providers should offer a persistent opt-out for first-party data collection and use, and obtain opt-in affirmative consent for the collection and use of sensitive information. The CDT also recommends that providers obtain opt-in consent for the default sharing of sensitive information with third parties.)

D) Sensitivity in LBS targeted to children and young adults

The use of mobile devices by children and young adults raises additional privacy and safety concerns. Indeed, a recent Carnegie Mellon study revealed that participants with children rated location-sharing technologies significantly more useful than those participants without children. That is to say, parents highly valued the check-in features of LBS-enabled applications but were also wary of risks associated with unsolicited advertising and unauthorized tracking by unwanted persons. Accordingly, it makes good business sense to be sensitive to consumer expectations as well as the extra legal scrutiny that often follows any marketing efforts targeted to young people. Businesses also need to be mindful of whether they are collecting location information from children under the age of 13 and the corresponding legal obligations that may be triggered under the federal children's privacy statute, the Children's Online Privacy Protection Act. Navigating through these legal obligations with a privacy expert is critical to avoid mishaps.

E) Stay current on privacy developments and resources
One common complaint by many businesses is that they were unaware a particular business practice was considered to be unlawful—a complaint that is generally made after a regulator or litigant initiates legal action. A practical tip: In the sometimes murky area of consumer protection and privacy law, the "rules of the road" often are gleaned from analyzing cases and law enforcement examples and expert resources on best practices rather than clear restrictions set forth in a particular statute. For this reason, it makes good sense to periodically monitor (adlawaccess.com) law enforcement actions that are announced by the FTC and state attorneys general that highlight privacy-related practices to avoid, as well as guidelines issued by organizations that focus on LBS and privacy issues.

Conclusion

If there are any 2012 predictions with favorable odds, they include the continued growth of LBS-enabled services and the commensurate examples of law enforcement against companies that engage in LBS without accounting for privacy developments. While privacy investment is not inexpensive, proactively implementing best practices at the outset is far less costly than being singled out by regulators, litigants and the media after the fact for privacy mishaps.

Alysa Zeltzer Hutnik is a partner in the Privacy and Information Security practice at Kelley Drye & Warren LLP in Washington, DC. She counsels on high-level domestic and global privacy, data security and related consumer protection issues, including those involving emerging technologies such as mobile apps, gamification and social media.
DoubleClick: The privacy profession's incubator

By Angelique Carson, CIPP/US

Today, it would be remiss to say that the privacy profession is anything but flourishing. Companies are increasingly hiring privacy officers and even elevating them to C-suite positions; the European Commission has proposed a statute in its amended data protection framework that would require data protection officers at certain organizations, and, at the IAPP, membership recently hit 10,000 worldwide.

But it's only in recent years that the need for privacy professionals has gained mainstream recognition. About a decade ago, privacy professional Jules Polonetsky, CIPP/US, recalls, one news publication—jabbing at the job titles dot-com's were coming up with—compared the title of "chief privacy officer" to "chief ninja."

"I remember the sarcasm," Polonetsky says. "They poked fun at what they thought would be an ethereal title."

But a firestorm surrounding one company's data collection practices put a spotlight on both privacy and the professionals tasked with protecting it, and out of that came a team of seasoned privacy pros who lived to tell the story.

Just over 10 years ago, Internet advertising agency DoubleClick announced that it would acquire direct marketing services company Abacus. The announcement incited criticism from privacy advocates and resulted in investigations by multiple federal and state agencies and litigators. Critics claimed the merger violated consumer privacy since it would allow for the combination of DoubleClick's data on users' online browsing habits with Abacus's database of consumers' offline personally identifiable information, such as names, addresses, ages and shopping habits.

One of those critics was the Electronic Privacy Information Center (EPIC), which filed a complaint with the Federal Trade Commission (FTC) in February 2000 alleging that DoubleClick engaged in "unfair and deceptive trade practices." EPIC called for the company to delete data it had collected from Internet users without their permission. DoubleClick's privacy policy at the time of the Abacus merger stated that it would not link the online and offline information, but a revised privacy policy soon retracted that claim.

In the heat of the firestorm, DoubleClick took action, hiring Polonetsky as its chief privacy officer and establishing a privacy advisory board. Polonetsky came to DoubleClick from his post as commissioner at New York City's Department of Consumer Affairs. He remembers the time period as one of both rapid change and success.

DoubleClick, Polonetsky says, believed it was truly providing value in helping pioneer Internet advertising, allowing websites to support cost-free content and helping advertisers transition into the digital age.

But the backlash that followed was unprecedented. It prompted a new look at privacy and the ways companies handled customer data.
It also carved out some career paths.

In fact, the team members Polonetsky assembled would become among the first and most high-profile privacy pros in the country as the media descended on the DoubleClick controversy and prodded for interviews with those on the front lines.

One of them was Nuala O'Connor Kelly, CIPP/US, CIPP/G, now chief privacy leader at GE, who came to DoubleClick in December of 2000 to serve as its first privacy counsel and then on Polonetsky's team. Elise Berkower would soon follow Polonetsky's path from the New York City Department of Consumer Affairs, where she worked as director of adjudication, to DoubleClick as a compliance officer.

Berkower says working in the privacy field at that time meant you were in a pretty small category and often circling around the same people. In fact, she calls DoubleClick the Kevin Bacon of companies—in reference to the small-world phenomenon that any Hollywood actor can be linked to Kevin Bacon within six degrees.

"You either worked there or you know someone who did," Berkower says.

Berkower arrived at DoubleClick shortly after O'Connor Kelly and was charged with checking all websites involved with online behavioral advertising and creating nonidentifiable profiles in order to retarget ads to them. She was also responsible for ensuring that websites' privacy policies complied. Brooks Dobbs would join as the company's technologist.

"There was a lot of pressure because we had to be ready for the audit, which was three or four months away," Berkower says. The first review was conducted by PricewaterhouseCoopers. Two additional audits were conducted by KPMG and two by Ernst and Young.

Dobbs was tasked with mapping personal identity information to the DoubleClick cookie and understanding who saw which ads. He'd been working in the online advertising business since 1994 and says, then, "we never considered that privacy would be an issue."

Arriving at DoubleClick, he says, he realized that the company had landed itself in the middle of a big issue.

"Once I got in there, I realized there's still sort of a dearth of understanding of where policy intersects with technical realities," he says.

For this early crew, it was a nerve-wracking time to blaze a trail.

During O'Connor Kelly's first three weeks at the company, she says, the FTC began an investigation, 21 class actions were filed and 12 attorney general investigations were launched.

"It was definitely the cutting-edge privacy and technology issue at that time," she says of the DoubleClick/Abacus investigation.

Adding to the intensity of the multiple investigations was the fact the case was unprecedented. There was no case law on the books or FTC decisions on privacy to turn to for guidance, O'Connor Kelly says. In fact, DoubleClick is listed as the first one.

"And it was a really pivotal time for Internet and e-commerce and privacy issues in particular--one that kind of brought privacy and data usage and handling into a much wider audience," she says. "I will be
really candid when I say we were making some of this up as we went along. To a certain extent, in the really early days, privacy officers were flying by the seats of our pants."

"These certainly were regulatory novel issues and new technological ideas that continued to be challenging to try to figure out how to deal with in a responsible way," Polonetsky agrees. "I certainly didn't know a great deal about privacy or data protection."

Berkower says, "The learning curve was very steep and the time was very short."

"We lived every day with an unexpected privacy scandal that someone was alleging or accusing," Polonetsky says. "From front-page stories about the White House being accused of having DoubleClick cookies tied to a campaign related to teaching teens about drugs to 60 Minutes stories to new class actions and lawsuits."

But the payoff for any privacy professional engaged in front-line issues like his team at DoubleClick faced, he says, is that "it can be a huge opportunity for a savvy CPO to get what he needs done accomplished."

"I think it was a crisis opportunity, and taking advantage of a crisis to really get the policies and people in place is how we were able to assemble a good team of people, and I think that's some of the lesson for other crises. Individuals dealing with the response need to strike while the iron is hot, whereas in non-crises situations, it can take time and convincing to get the right policies and people in place," Polonetsky says.

The FTC eventually would close its DoubleClick investigation, ruling that the company had not violated its privacy policy.

"I remember when we got the letter that the case had been closed," O'Connor Kelly says. "What an exciting time."

And in the meantime, she adds, a new profession was born.

"I think the takeaway for me is that it helped me be a part of a team that built the structure of privacy, which is something I've replicated almost everywhere I've been."

What's next?

Dobbs says it will be interesting to see where the issue at the heart of the DoubleClick controversy ends up.

"We're 10 years into it, but as a business model, it's sort of ancient," he says. "We haven't figured out how to make money doing this, and there's this battle on the one side to create an advertising mechanism that generates enough utility to pay for expensive content, and on the other side, there's this growing unease about the data that's being collected. And those are pushing in opposite directions."

He says the question will become "do you, consumer, want to start giving up more data about yourself and get content for free? Or, alternatively, are you going to be part of the tragedy of the commons and exert your right to not permit data collection, and eventually run the pumps dry?"

Polonetsky says that over the years, his opinions on privacy have continued to evolve, but they've always centered around one core principle.
“Are you treating people fairly here? Because it's about treating people really well,” he says. "If you want to make money doing things for people, treat them really well."
Privacy pro garners all five CIPP certifications

By Jedidiah Bracy, CIPP/US, CIPP/E

Since its inception in 2004, the Certified Information Privacy Professional (CIPP) credential has served as the leading certification for privacy professionals. Like the IAPP’s membership, the CIPP credential has grown more diverse over the years. The IAPP’s flagship credential has developed into multiple credentials, including one focused on the U.S. government, Canada, Internet technology and now Europe.

The IAPP’s newest designation—the CIPP/E—was rolled out at the Data Protection Congress in Paris last November. In a year that has seen the unveiling of the European Commission’s draft data protection rules, the CIPP/E has become the newest and hottest designation for aspiring privacy professionals.

Last December, Accenture North American Director of Legal Services and Data Privacy Compliance Benjamin Hayes, CIPP/US, CIPP/G, CIPP/C, CIPP/IT, CIPP/E, became the first privacy pro to achieve all five designations.

Clearly, Hayes is steeped in a wide range of privacy knowledge. Not only does he act as both a legal and business advisor, he is a product designer, a crisis manager and an educator. Hayes is responsible for internal compliance with privacy laws, supports client and supplier contracting, doles out expertise for Privacy by Design projects, specializes in privacy legal compliance for cloud computing and has created training and education for data protection issues.

A former student of privacy scholar Peter Swire, CIPP/US, Hayes has been a privacy lawyer since 1999—his entire legal career.

The Privacy Advisor recently caught up with Hayes to discuss his five CIPP designations, what they mean for his job and aspiring privacy professionals and what achieving a “blackbelt” in privacy might mean.

The Privacy Advisor: You take on a lot of different roles in your position. How have the IAPP certifications helped you on the job?

Hayes: Internally, a number of my many roles are relatively new to the business, and so any sort of external validation that I and my team actually know what we’re doing helps to build confidence and trust with our internal clients. At the same time, these effects are limited because most people outside the privacy world don’t really know what the IAPP is or what holding a CIPP means. But within the privacy world, it’s extremely valuable, because privacy people do pay attention to these things. Our company hosts or has access to many other companies’ sensitive data, and it is critical that we understand how to properly manage that responsibility. I believe it helps Accenture when privacy professionals at our client companies see our team’s commitment to understanding data privacy issues and pushing forward in the area. Accenture was also the first company to achieve EU-wide recognition of our Binding Corporate Rules. We are continually striving to have the best privacy and data protection programs in the world.

The Privacy Advisor: What would you say to someone who is early in their career, or switching careers, and is considering an IAPP certification?
Hayes: One of my mantras is that a privacy professional’s first job is to actually be an expert. You absolutely have to have the substantive knowledge of law, regulation, technology and trends to be effective in this area. CIPP certification has become—to the IAPP’s credit—de rigeur in order to be taken seriously as a privacy professional, so at a basic level, it is a prerequisite to privacy as a career path. It can also be a good learning vehicle for people new to the area. While there isn’t any substitute for the experience of applying privacy laws to real-world situations, studying for and passing the CIPP Foundation exam will at least give people who are new to the area a basic overview of what they should be thinking about.

CIPP certification doesn’t, of course, make someone an effective privacy professional—it’s more of an indicator. There are a number of skills that privacy professionals need—e.g., the ability to communicate clearly, to educate and to serve as agents of institutional change—that the CIPP exams don’t measure. I see CIPP certification as more of a starting place, a minimum standard for who gets to call themselves a privacy professional. Even my five certifications don’t mean much in and of themselves, but they are at least an indicator that I have spent time thinking about a range of data privacy issues and, hopefully, that I am committed to privacy as a profession. The IAPP has done a great service by establishing some minimum standards for privacy professionals, but it could go farther. I can imagine new CIPP certifications for health, financial services, etc.—and yes, I will get those too—but beyond that, I’d really love to see some sort of “master-level” certification that would serve as sort of a privacy blackbelt. CIPP sets a good basic benchmark of knowledge, but I think it would be great if there was a high bar as well.
FRANCE—The French Senate issues a resolution to express its position on the draft European regulation for the protection of personal data

By Pascale Gelly, CIPP/E, and Caroline Doulcet

The Senate, in its European resolution of March 6, welcomes the objective of harmonization of data protection rules as well as additional guarantees, such as the right to be forgotten, data portability, limits to profiling activities and a mandatory data protection officer.

However, the Senate considers that these guarantees must be strengthened. An automatic deletion of indexed personal data after a certain time should be required from search engines. Moreover, data subjects should have the right to ask for the deletion of damaging contents, in compliance with the right of freedom of speech. The IP address should be characterized as personal data each time it is used to identify an individual. Also, the appointment of a data protection officer should be mandatory for companies whose main business consists in carrying out data processing activities.

Besides, the Senate points out the measures raising concerns with respect to the level of data protection in the European Union:

- The prominent powers of the European Commission concerning the application of the European regulation and the residual role of member states and Data Protection Authorities (DPAs) are challenged by the Senate. This operating mechanism is considered as not being in line with the objective of ensuring a high data protection level within the European Union. The Senate claims for member states to have the possibility to enact rules more protective than the European regulation when necessary;

- The rule of the jurisdiction of the DPA of the main establishment, when a company located in the European Union carries out data processing in different member states, is considered as protective only for companies but not for individuals, who will be deprived of the benefits of having their claim handled by the DPA of their own country;

- The requirement for a DPA to have a reasonable reason to suspect that a data controller is in breach, for investigating is considered as inappropriately limiting the DPA’s investigation power. Indeed, investigating will be the only way for DPAs to verify compliance of data processing when companies will be exempted from prior formalities with the DPA.
This European resolution is globally in line with the resolution adopted in February by the National Assembly.

*Pascale Gelly, CIPP/E, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.*

*Caroline Doulcet, of the French law firm Cabinet Gelly, can be reached at cd@pascalegelly.com.*
FRANCE—Disparaging one’s manager in a private e-mail does not justify termination

By Pascale Gelly, CIPP/E, and Caroline Doulcet

An employee sent an e-mail to a colleague including a fictitious CV with denigrating comments about his manager. The “friendly” colleague transmitted the litigious CV to the concerned manager, who made a case out of it, leading to the termination of the author of the fictitious CV for serious misconduct.

The whole case revolves around the characterization of the e-mail as private or not, whereas the sender and the recipient were employees of the same company, the subject matter was a manager and the content went beyond what would be tolerated by freedom of speech.

Contrary to the Court of Appeal, the Supreme Court characterized the litigious e-mail as private. It noted that the e-mail had not been sent from the work place or during working hours. Also, it had been sent from the private e-mail box of the fired employee to the private e-mail address of the colleague. As a result, sending this e-mail did not constitute a breach to the fairness obligation of the employee and could not justify a dismissal for serious misconduct.

Pascale Gelly, CIPP/E, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.

Caroline Doulcet, of the French law firm Cabinet Gelly, can be reached at cd@pascalegelly.com.
ISRAEL—New guidelines for employees' placement services

By Dan Or-Hof, CIPP

The Israeli Law Information and Technology Authority (ILITA) has published new guidelines on privacy principles for applying the provisions of the Protection of Privacy Act on jobs placement services.

The guidelines are a result of a four-year process of consultations led by ILITA with placement services, employers and other relevant stakeholders. Their main objective is to enhance the privacy protection of job applicants in an environment where they have little if any choice with respect to the processing of their personal information.

Under the guidelines, the employer is the owner of the data that the placement service collects and processes at the employer's request. The placement service is the holder of that database. According to the Privacy Protection Act, as the holder of the database, the placement service does not have any rights to process the data for any purpose other than the purposes that the employer defined. Therefore, a placement service may not transfer such data to another employer without separate and specific consent of the applicant.

ILITA regards the placement services as outsourcing services. Therefore, the employer must make sure that the placement service agreement is in line with ILITA's guidelines for outsourcing the processing of personal information.

If a placement service holds data for multiple employers, then it must make sure that every employer has access to data that is relevant to that employer only. A placement service that holds information for five or more employers must appoint an information security supervisor.

The guidelines further provide that an applicant cannot waive the right to view data related to that applicant and held by the placement service and the employer. Generally, placement services and employers must allow the applicant access—without any cost—to an exact copy of the placement service's opinion of that applicant. However, an applicant can provide a prior informed consent to limit the scope of the right to review the data, if the applicant is likely to suffer from a mental injury because of being exposed to that data, or if the data contains confidential information of the placement service or of the employer.

The Protection of Privacy Act does not contain any explicit data retention provisions. However, ILITA believes that the prohibition on processing information for a purpose other than consented purposes forms a de facto data retention provision. It follows that the employer and placement service must destroy or anonymize the data about that applicant immediately after the use of the data for the placement process has ended. The above prohibition does not prevent employers from keeping opinions in an archive for lawful purposes under strict “need-to-know” access arrangements. Additionally, employers may keep a copy of the opinion in the employee's personal file.
The guidelines were published on February 28, and they take effect immediately.

A copy of the guidelines (in Hebrew) is available on ILITA's website.

Dan Or-Hof, CIPP/US, is a New York and Israeli attorney, a partner and the manager of the IT, Copyright and Internet team at Pearl Cohen Zedek Latzer, with specific practice in data protection and privacy law.
UK—Data watchdog routinely reducing data breach fines

By Olivia Harrisson
Since April 2010, the Information Commissioner’s Office (ICO) has had the power to impose fines of up to £500,000 for serious breaches of the DPA.

To date, the ICO has issued 14 fines, but information obtained by Out-Law.com under a freedom of information request indicates that the final penalty is often substantially reduced. In one case, a £200,000 penalty imposed on a lawyer, Andrew Crossley, was reduced to just £1,000 after Crossley filed for bankruptcy. A further four cases revealed an average reduction of around 20 percent in the value of the fine the ICO had originally considered.

When considering what fine to impose, the ICO considers the severity of the breach and any representations made by the data controller—with the data controller’s ability to pay being one of the factors the ICO will consider. Data controllers are therefore well-advised to consider what representations they can make to the ICO to minimise the value of any potential fine they face.

UK—Jail terms for private detectives convicted of blagging

By Olivia Harrisson
Four private detectives convicted under the Fraud Act of stealing confidential information for sale to clients have been sentenced to jail terms of between six and 12 months.

While the information commissioner welcomed the sentences, he renewed his call for custodial sentences to be put in place for offences under section 55 of the Data Protection Act 1998 (DPA). At present, Section 55 offences—unlawfully obtaining personal data—are not punishable by imprisonment and, if this case had been pursued under the DPA, the individuals convicted would have faced only a small fine.

Describing this situation as "not good enough," the information commissioner expressed concern that “blagging” offences would continue unabated until the punishments available under the DPA “fit the crime.”

UK—CBI critical in response to MoJ consultation on EU data protection reforms

By Olivia Harrisson
On 7 February, the UK Ministry of Justice (MoJ) published a Call for Evidence to gather information from interested parties, including businesses and information policy experts, on the European Commission’s draft General Data Protection Regulation.

Unveiled on 25 January, the proposed regulation marks a significant legislative development in the global collection, use and protection of personal information, and the MoJ will use the information gathered from this exercise in forthcoming negotiations on the European Commission’s proposed reforms.
The CBI, a high-profile business lobbying organisation in the UK, has criticised the reforms, saying that the high costs of compliance and legal uncertainty will "stifle innovation and deter investment." In its response to the MoJ's Call for Evidence, the CBI also pointed to the potential for "poorly defined rights" to cause problems for consumers, regulators and businesses.

The Call for Evidence closed on 6 March and results are expected to be published on 4 June. A copy of the CBI's response is available on the CBI website.

UK—ICO issues police force with £70,000 fine

By Olivia Harrisson
Lancashire Constabulary has been fined £70,000 by the Information Commissioner's Office (ICO) following the discovery of papers containing sensitive information about a 15-year-old girl—together with information about 14 other individuals, including in relation to their criminal convictions—on a Blackpool street.

In July 2011, a member of the public discovered the missing persons report containing the girl's name, age, contact information, sexuality and information about a rape suffered by the girl, and handed it to a local newspaper. It is believed the information fell out of a police car used to attend an incident the day before.

The ICO's investigation found that the removal of sensitive personal information from police stations was not recorded, secure bags were not provided for the storage of this information and that officers did not receive training about protecting hard copy documents outside the police station.

BIO NOT APPROVED

Olivia Harrisson is a trainee solicitor with Field Fisher Waterhouse’s Privacy and Information Law Group. She can be reached at Olivia.Harrisson@ffw.com.
PCI-DSS Version 2.0 comment period coming to a close

By Angelique Carson, CIPP/US

The Payment Card Industry (PCI) Security Standards Council will soon conclude its public comment period on version 2.0 of the PCI Data Security Standard and Payment Application Data Security Standard (PCI DSS). The council, a global, open industry standards body for the PCI DSS, began soliciting comments in November of last year from its members and other parties.

Version 2.0 increases the granularity of the standard from version 1.0’s vague language and parameters, according to Paul Nowling and Rick Heroux of Compliance Solutions and Resources.

The council “took things that were not clear and people were not doing and broke the requirements down into what the real expectation is,” Heroux said, adding that version 2.0 “significantly improved merchants’ abilities to be compliant.”

One major improvement was the advent of the SAQ C-VT, an abbreviated self-assessment tool that helps small- and medium-sized merchants that have trouble getting through the longer, more complex questionnaires that may have not even applied to them become compliant. Heroux said version 2.0 has clarified requirements for merchants and “brought it down to a level to what they needed to do to protect specifically what they were doing on these machines.”

He added that merchants that tend to struggle the most, to date, are those that have a complex but easy-to-use system—a point-of-sales system, for example—that requires technical knowledge and security; those who allow vendors access to passwords without realizing the danger of third-party access to data, and those with a lack of awareness about the danger of out-of-box default passwords that can generally be found online and should be changed immediately.

The standards are updated every three years based on such feedback, and the feedback periods are launched one year from the time new standards are issued. PCI DSS version 2.0 became effective as of January 1, 2011.

Revising standards according to feedback is essential, Nowling said, because it only encourages compliance.

“The last thing you want to do is get a merchant started on a process and have it so complicated that they throw their hands up and walk away,” Nowling said, “Because even if they couldn’t meet all requirements, there is so much to be gained from having a policy and from training employees. The majority of breaches come from employees not being trained and hooking up to a point-of-sale system.”
Former DHS Deputy CPO John Kropf, CIPP/US, CIPP/G, joins Reed Elsevier

Reed Elsevier Group has announced the addition of former Department of Homeland Security (DHS) Deputy Chief Privacy Officer John Kropf, CIPP/US, CIPP/G, to its privacy and information governance group.

"By hiring John, an experienced and respected member of the global privacy community, Reed Elsevier is reinforcing its commitment to being a global leader in privacy, data security and information governance," said Reed Elsevier Intellectual Property, Privacy and Governance General Counsel Ken Thompson.

Kropf brings more than 20 years of government experience to his new role as the principal contact on privacy matters with the Federal Trade Commission, other government agencies and the greater privacy community, according to Reed Elsevier’s announcement.

"Reed Elsevier is committed to being a global industry leader on privacy. The opportunity to join their team to provide a center of excellence on privacy and information governance is a perfect fit with my background," Kropf told The Privacy Advisor. "I look forward to continuing and strengthening their privacy practice across all of their business units."

Reed Elsevier Group is a provider of professional information solutions to the science and medical, legal, risk management and business-to-business sectors with 30,000 employees, including 16,000 in North America.

— IAPP Staff
Ellen Giblin, CIPP/C, CIPP/G, joins Ashcroft Law Firm

Ashcroft Law Firm LLC has announced the addition of Ellen Giblin, CIPP/C, CIPP/G, as privacy counsel. Working primarily in the firm’s Boston, MA, office alongside former U.S. Attorney Michael J. Sullivan, Giblin will contribute to the areas of privacy, data protection and cybersecurity challenges.

“These topics can be among the most difficult issues that companies face today, in part because privacy, data protection and risk management are evolving areas and because technology and the ways we use personal information is changing at incredible speed,” Giblin said, adding, “It’s vital that companies address these issues imminently, and I look forward to helping the firm’s clients meet the challenges not just of today but of the future as well.”

Giblin brings more than 25 years of experience advising multinational and domestic clients on privacy and data protection, including regulatory risk and data breach response.

Former U.S. Attorney General John Ashcroft, chairman of the firm, said in the announcement of Giblin’s addition that she “greatly enhances our existing practice in data security, risk management and cybersecurity. Clients of the Ashcroft Law Firm will be able to improve substantially their security and compliance posture with the benefit of Ellen Giblin’s extensive experience and that of our team.”

Sullivan said Giblin “brings a wealth of experience and knowledge that will be of immediate value to both domestic and international companies as they attempt to protect information and property and meet the complex and ever-changing regulatory requirements both here and abroad.

— IAPP Staff
More than 2,100 privacy professionals descended on Washington, DC, in March for the 2012 IAPP Global Privacy Summit.

View Photos
(Must be a Facebook user and logged in to view.)