E-Discovery in Asia/Pacific:
U.S. litigation exposure for Asian companies

By Thomas Shaw, CIPP

This is the second article in a three-part series exploring litigation exposure and readiness for Asian companies. Here, Thomas Shaw explores how Asia/Pacific-based companies can analyze and deal with the risks of U.S. litigation exposure to pre-trial discovery data requests. Part three will review the principles of the APEC Privacy Framework, comparing Asian countries’ privacy laws to those principles and suggesting a model set of corporate privacy principles.

Due to expansive rules on discovery, jury trials and the size of damage awards, plaintiffs worldwide would choose to bring their claims, if possible, in U.S. courts. As such, when non-U.S. companies are performing their periodic risk analyses, they must consider their exposure to U.S. litigation, either directly or through their U.S. subsidiaries. Having such exposure means being potentially subject to liability for damages but even more likely subject to pre-trial discovery requests for paper documents and electronically stored information (ESI) (collectively “data”) under the control of the non-U.S. company. This article focuses on how non-U.S. companies, particularly those based in the Asia/Pacific region, can analyze and deal with the risks of U.S. litigation exposure to pre-trial discovery data requests.

Non-U.S. parent corporations should already understand that their subsidiaries operating inside the U.S. have exposure to U.S. litigation, either through the well-established principles of personal jurisdiction or through forum selection clauses in contracts. What is not as well understood is that non-U.S. parents themselves may also have exposure to U.S. litigation pre-trial discovery requests. The U.S. Federal Rules of Civil Procedure (FRCP) used to guide
See, E-discovery in Asia/Pacific, page 3

The ethics of “Googling” someone

By Christopher Wolf

Just because you can “Google” someone, should you? This is a good question for the U.S. Federal Trade Commission, which is re-examining privacy during a series of roundtable events this winter.

One would not expect a Supreme Court Justice to weigh in on the question unless it was presented formally before the Court. But the absence of a case did not stop Justice Antonin Scalia from expressing his opinion that searching online for personal details about someone—him—is wrong. What prompted the Justice’s pronouncement? Fordham University Professor Joel Reidenberg assigned his privacy class to “Google” Justice Scalia and his family (and look at other publicly available sources), as an educational exercise to show just how much information is out there on the Internet about each of us. The search turned up family pictures, home phone numbers, and other Scalia family information not intended for the world at large. Professor

See, Ethics of Googling, page 15
December • 2009

Notes From the Executive Director

Our first issue of the Advisor every year has always been about looking forward into the New Year. What will change in the privacy world? What new laws and regulations will challenge privacy pros? What major media stories—whether breaches, emerging technologies, or boundary-stretching business models—will strain our current tools for managing data? There are always more questions than can possibly be answered.

Next month’s issue will be packed with the predictions of privacy pros and luminaries. Until then, permit me to gaze into the cloudy crystal ball of privacy, fully understanding that predictions are always a risk—and frequently prove embarrassing when viewed with the clarity of hindsight.

It is difficult to argue that privacy has only grown in significance in the past 12 months. And, looking forward, we have to assume that the issues we grapple with daily will only continue to expand. In 2010, we can expect further discussions of the EU Data Protection Review, an FTC staff report on the heels of the “Exploring Privacy” roundtable series, and an oft-predicted privacy bill in Congress. But we knew these things already. What else might challenge us in 2010?

Make sure you keep your eyes on the U.S. Supreme Court, which will decide the Quon case in the first half of the year. This case has the potential to throw asunder the status quo of employee privacy in the U.S. The case deals with the murky intersection of employer-provided technology and the reality of a converged work/home lifestyle. The legal and social aspects of Quon make the privacy issues particularly fascinating.

Watch for a proliferation of symbols, icons, and novel notices to try to communicate data practices to the marketplace. Privacy pros are doing some incredible work in this space—with the Future of Privacy Forum and others pushing our current thinking about notice in helpful new directions. It is unclear which, if any, of these ideas will gain traction. But it is certainly encouraging to see the level of innovation.

Be prepared for continued acceleration in the debate over consumer privacy online. Many regulators around the world—including the FTC, Canada’s privacy commissioner, and various EU data protection authorities—are continuing to look closely at social networking, online video postings, street imaging services, and behavioral advertising. Some of these debates are near a breaking point, where new standards will emerge or business models will be forced to change. More aggressive enforcement in this space is certainly a possibility as well.

Expect continued growth in the size and sophistication of the privacy profession. In 2009, the IAPP grew 20 percent in membership. When considered against the backdrop of the economy, that growth is nothing short of astounding. In 2010, as the market begins to loosen up, we can certainly expect that more privacy pros will be hired to respond to the myriad issues our profession manages.

And I would be remiss if I did not mention that, in 2010, the IAPP will be celebrating its 10th anniversary. Hard to believe, but our organization has been around for a whole decade! So my safest prediction is that the IAPP will be gathering members around the world to recognize how far we have come as a profession in these few years. We certainly have a lot to celebrate.

J. Trevor Hughes, CIPP
Executive Director, IAPP
U.S. civil litigation only give the responding party about 100 days to be able to fully describe their data that is responsive to a lawsuit. As such, non-U.S.-based parent corporations need to proactively evaluate their litigation exposure risks and if so exposed, prepare themselves well in advance to be able to respond quickly and fully to pre-trial discovery requests for the production of responsive corporate data.

When performing such a risk analysis for U.S. litigation discovery exposure, a non-U.S. corporate parent with U.S. subsidiaries must answer the following four questions:

- Will U.S. pre-trial discovery take place under U.S., international, or local rules?
- Will U.S. courts have the power to order a non-U.S. corporation to produce data?
- Will U.S. courts order discovery if there are local data protection laws in place?
- What additional factors will U.S. courts consider for discovery of overseas ESI?

Procedural rules

Under the U.S. FRCP (and similar state rules), a party to a lawsuit may request the other party or a non-party to produce data. This data can involve “any non-privileged matter that is relevant to any party’s claim or defense.” The responding party may voluntarily reply to these requests but if it does not, the initiating party may request a court order compelling discovery. To issue such an order, the court must have personal jurisdiction over the party who will be compelled and that party must have control of the documents (see following section). But for responding parties located outside the U.S. who control data that is the subject of a discovery production request, the court may have to consider a second set of procedural rules available from the Hague Conference on Private International Law.

The Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the “Hague Convention”) is a multilateral agreement detailing procedures for requesting evidence from the authorities in another country. Almost 50 countries are currently signatories, including the U.S. Both the FRCP and the Hague Convention are considered the law of the United States. Under the Hague Convention, to obtain evidence in the other signatory country, a letter of request is transmitted to that country’s Central Authority for execution. In Aerospatiale, the U.S. Supreme Court ruled that the Hague Convention is intended as an optional supplement to obtain evidence located abroad, as opposed to the exclusive procedure for requesting such evidence. The determination of whether the Hague Convention should be utilized is based on these three factors:

- the particular facts of each case;
- the sovereign interests of the respective countries;
- the likelihood that the Hague Convention procedures will prove effective.

A party wanting to utilize the Hague Convention has the burden of persuasion regarding its use instead of the FRCP. Article 23 of the Hague Convention allows signatories to pass laws to refuse to comply with common law discovery requests. In Asia/Pacific, only four major countries are signatories of the Hague Convention (Australia, China including Hong Kong and Macau, India, and Singapore). Each of these countries has taken an Article 23 reservation, meaning that letters of requests for discovery will not be executed by the local officials. Only China for itself (not Hong Kong or Macau) states that it will execute a letter or request that has a “direct and close connection with the subject matter of the litigation will be executed.” Even then, it may not be effective.

See, E-discovery in Asia/Pacific, page 4
E-discovery in Asia/Pacific

continued from page 3

timely as, according to the State Department, “while it is possible to request compelled evidence in China pursuant to a letter rogatory or letter of request (Hague Evidence Convention), such requests have not been particularly successful in the past. Requests may take more than a year to execute.” Hong Kong, Macau, Australia, India, and Singapore will not even execute a letter of request for purposes of obtaining pre-trial discovery of documents. Australia’s declaration is typical of these: “pursuant to Article 23, [we] will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in common law countries.” As such, a responding party from an Asia/Pacific signatory country is unlikely to persuade a U.S. court to use the Hague Convention.

For parties based in all other Asia/Pacific countries who are not Hague Convention signatories, a U.S. court would likely determine whether the FRCP or local rules of discovery would be used, based on two steps: first to determine whether a conflict exists between the two sets of procedural rules and second to perform a comity analysis. The comity analysis, endorsed in Aerospatiale and based on the Restatement (Third) of Foreign Relations Law §442(1)(c), uses the following five factors:

- importance to the litigation of the information requested;
- degree of specificity of the discovery request;
- whether the information originated in the U.S.;
- availability of alternate means of securing the requested information;
- extent to which non-compliance would undermine important interests of the U.S. or compliance would undermine important interests of the other country involved.

Other courts have used additional factors, such as hardship, on the responding party if facing criminal sanctions for producing the data or a non-party status. In In re Vitamins, because it is not a Hague Convention signatory, Japan’s Code of Civil Procedure Law was analyzed and a conflict was found between the local law and the FRCP. Then the comity analysis found that the local procedural rules would not allow for a “prompt and efficient resolution” and so the court ordered discovery to proceed under the FRCP instead.

Jurisdiction and control
A U.S. court can order a non-U.S. parent corporation to produce data if the court:

- has personal jurisdiction directly over the non-U.S. parent;
- can acquire personal jurisdiction over the parent indirectly through a U.S. subsidiary;
- determines the subsidiary has control over or access to the non-U.S. parent’s data.

Personal jurisdiction directly
A U.S. court must have personal jurisdiction over the responding party against whom production of the relevant data is sought under pre-trial discovery. The standard analysis is under “minimum contacts,” requiring the responding party to have a certain minimum level of contacts with the forum the court is situated in, as first described in International Shoe. The minimum contacts analysis under local statutes allows for jurisdiction that is either “general” or “specific.” General jurisdiction will support “a suit not arising out of or related to defendant’s contacts with the forum” if the respondent has continuous and systematic contacts with the forum. Specific jurisdiction will support “a suit arising out of or related to the defendant’s contacts with the forum” when the defendant has purposefully availed itself of the benefits of the forum. In addition, the result must comport with due process in that it is reasonable and with sufficient notice.

Under either general or specific jurisdiction, a U.S. subsidiary of a non-U.S. parent corporation doing business within the U.S. would likely come under the jurisdiction of the U.S. courts. A non-U.S. parent corporation that is doing business directly through a U.S. branch office would also. But would the non-U.S. parent corporation itself fall under the jurisdiction of U.S. courts if only its subsidiary, not the parent, is doing business in the U.S.?

In Asahi Metals, the U.S. Supreme Court held that placing products into the stream of commerce was not sufficient contacts for personal jurisdiction over a non-U.S. (Japanese) corporation. In other cases, personal jurisdiction over non-U.S. corporations has been found. Finding of personal jurisdiction over a parent corporation under a minimum contacts analysis is very fact-specific and must be uniquely determined in each situation.

Personal jurisdiction indirectly
If minimum contacts between the non-U.S. parent corporation and the U.S. forum are not found, jurisdiction over the parent can still be found by looking through its U.S. subsidiary and “piercing the veil” of the parent’s U.S. subsidiary. This can apply not only when the subsidiary was set up for fraudulent or illegal purposes, but also for a legitimately organized subsidiary, depending on which of three different lines of cases, as articulated in Gallagher, is used.

One precedent, termed the Cannon line of cases, holds that only by creating and then not respecting the parent/subsidiary legal differences is jurisdiction over a parent gained through a subsidiary. A second precedent, the Scophony line of cases, holds that personal jurisdiction over a parent may be possible if based on the extent of control the parent exerts over the subsidiary, to the point of dominating the subsidiary’s operations. This looks to factors including common ownership, financial dependency of the subsidiary, the parent’s interference with subsidiary executive selection, and the parent’s control over the subsidiary’s marketing and operational policies. A third precedent, the Gallagher line of cases, allows
jurisdiction over a parent if a subsidiary engaged in functions that the parent would have to otherwise undertake. As stated by the court in Bulova Watch, if a subsidiary is expanding a parent’s market position in the forum, then the parent is doing business in the forum.

An analysis of the parent/subsidiary relationship should consider at least the following:

- Is the subsidiary adequately capitalized?
- How sufficiently are the corporate formalities observed?
- What level of control does the parent maintain over the subsidiary’s operations?
- Are there separate bank accounts?
- Are parent-subsidiary loans at market rates of interest?
- Is the subsidiary insured?
- Is the subsidiary 100 percent owned and are there interlocking directorates?

**Control or access**

Once personal jurisdiction over the non-U.S. parent has been established, a party may seek production of data in its “possession, custody, or control.” A U.S. court has the power to require the production of data located in foreign countries if the court has personal jurisdiction over the corporation in possession or control of the data. But if personal jurisdiction over a non-U.S. parent is not established, a court may still order production of data held by the non-U.S. parent through its U.S. subsidiary.

In *In re Uranium Antitrust Litigation*, the court looked at a number of factors to determine if a U.S. subsidiary had “control” over the documents held by its non-U.S. parent. These factors included the percentage of ownership of the subsidiary by the parent and the management unity of the two companies. The court noted that the ability to compel production of data and liability for a subsidiary’s acts is distinct and that the corporate formalities cannot be “used as a screen.” Other courts have also allowed access to data held by the parent corporation, even though jurisdiction was held only over the subsidiary.

In *Linde*, the court stated that a party attempting to compel a U.S. subsidiary to produce documents of its foreign parent has to show the documents were within the subsidiary’s control. Control is inclusive of: possession, the legal right to obtain documents and access to and the ability to obtain documents. This control could be shown where documents “ordinarily flow freely between parent and subsidiary” or where it could “generally obtain documents” from its non-U.S. parent to assist itself in litigation. The court held there was no control, using these factors plus the fact that the parent and subsidiary shared no computer systems or confidential customer transaction information.

**Data protection laws**

Once a court has established the power over data held by a non-U.S. parent corporation, the court must then determine if it should use that power in the face of any data protection laws that may exist in the country of the parent corporation. Countries across the world have a variety of data protection laws, in the form of secrecy laws, privacy statutes, and blocking statutes. Commercial secrecy laws typically protect corporate and banking data. Privacy statutes typically protect consumers and their personal information. Blocking statutes have typically been enacted for the express purpose of frustrating U.S. discovery.

**Caselaw**

In *Societe Internationale*, the U.S. Supreme Court stated that the responding party cannot fail to produce documents because of a foreign data protection statute. The Court outlined three factors that should be considered when it is determining whether to exercise its power to order discovery in the face of a non-U.S. data protection law:

See, E-discovery in Asia/Pacific, page 6
E-discovery in Asia/Pacific

continued from page 5

• the strength of the policies underlying the U.S. statute;
• whether the requested data are crucial to resolving a key issue in the lawsuit;
• the amount of flexibility in the application of a country’s data protection law.

Each factor requires additional explanation. The first factor does not balance the U.S. statute against the data protection statute of the foreign country but only considers the U.S. statute. The second factor is actually a higher standard than the typical U.S. standard for production of data during discovery, which is any data that is relevant or could reasonably lead to admissible evidence. The third factor speaks to the ability of the responding party to deal with its own government in trying to waive enforcement of the data protection law and whether it has done so. The good faith of the responding party is not considered when ordering production, but only after an order is not complied with.

In cases that followed, the majority of U.S. courts have not allowed blocking statutes to stop the issuance of production orders. In In re Vitamins Antitrust Litigation, the court stated that it is well settled that blocking statutes do not deprive the U.S. courts of power to order a party to produce evidence even though the act of production may violate that statute. To some extent, this was because U.S. courts did not believe that the sanctions attached to these blocking statutes would be enforced. This may have changed with what happened after a discovery production order was issued in face of the French blocking statute. A French attorney who subsequently tried to speak to a witness in contradiction of the blocking statute was convicted and fined in a result that was upheld by the French Supreme Court. The subsequent effect of this on the analysis by U.S. courts is not yet clear.

After evaluating local secrecy and privacy laws, courts have still ordered discovery anyway. In Societe Internationale itself, the Court ruled that the Swiss banking secrecy law was not sufficient to prevent ordering production of data from the respondent. In Richmark Corp., China’s secrecy law was not allowed to protect the financial information of a state-owned company. In First National City Bank, the court upheld production because Germany’s bank secrecy law was waive-able and only civil penalties and commercial consequences were likely to result. In In re Uranium Antitrust Litigation, the court held that discovery was required of respondents despite data protection laws from three different countries, each with widely differing amounts of flexibility in enforcement of those laws.

Asia/Pacific data protection statutes

In Asia/Pacific, there are quite a range of statutes set up to protect various types of data. These statutes serve various segments of society, from consumers to business to government. These local

PrivacyAdvisor

Eliminate 100% of your compliance risk across all channels, guaranteed.

Gryphon’s on-demand, contact governance software solution is the easy answer to your customer contact challenges. PrivacyAdvisor uses a simple traffic light visual to manage contact compliance, and streamlines every step of the sales and marketing process. It also:

- Ensures 100% compliance across all channels
- Seamlessly integrates with salesforce.com and Oracle CRM On Demand
- Certifies contacts in real time
- Prevents costly fines and PR nightmares
- Expands your marketable universe up to 60%

Get the green light on multichannel contact management. Call or click today.

Wouldn’t it be great if DNC compliance was this simple?

With PrivacyAdvisor, it is.
laws should be part of the legal risk analysis for parent corporations but it is important to understand that each statute has not been interpreted by a U.S court. In addition, many statutes are being updated or introduced as this article is being written, so any risk analysis must be constantly revisited. In addition to statutes, there are also regional frameworks, such as the non-binding APEC Privacy Principles, that may have a greater influence in the absence of local privacy law or on future statutes. The following is a non-comprehensive but representative list of regional data protection laws.

See, *E-discovery in Asia/Pacific*, page 8

<table>
<thead>
<tr>
<th>Regional Data Protection Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Australia:</strong> The Foreign Proceedings Act of 1984 is a blocking statute for common law discovery. The Federal Privacy Act of 1988 (revised in 2001) that lays out ten National Privacy Principles, which includes a requirement to have a reasonable belief and take reasonable steps that any personal data transferred outside the country be to a recipient that upholds the National Privacy Principles. Australia also protects commercial secrets under the general law concerning confidentiality.</td>
</tr>
<tr>
<td><strong>China:</strong> The State Secrecy Law is implicated when any information is deemed by the Chinese government to be a state secret, which may include civil matters when the government is involved (e.g. as an owner). The Unfair Competition Law is for the protection of commercial secrets. A Data Protection Law has been in development for the last several years.</td>
</tr>
<tr>
<td><strong>Hong Kong:</strong> The Personal Data (Privacy) Ordinance of 1995 has a provision for the onward transfer of personal data that requires that there be a reasonable belief that any personal data transferred outside Hong Kong without consent is transmitted only to a recipient operating under similar privacy laws. Bank secrecy is contractual instead of statutory.</td>
</tr>
<tr>
<td><strong>India:</strong> Article 21 of Constitution has been interpreted by the Indian courts to include a right of privacy. The IT Act of 2000, based on the model U.N e-commerce law, was revised effective in 2009 and has select privacy provisions.</td>
</tr>
<tr>
<td><strong>Japan:</strong> The Personal Information Protection Act of 2003 protects personal data and does not allow un-consented transfers of personal data to third parties, with the exception of certain outsourcing companies (e.g. payroll processing). It also has notice and opt-out provisions. Japan protects commercial secrets under the Unfair Competition Prevention Act.</td>
</tr>
<tr>
<td><strong>Singapore:</strong> There is a voluntary privacy framework, the Model Data Protection Code for the Private Sector, which applies to any recipient to whom personal data is transferred, in or outside the country. Singapore’s Banking Law states that “customer information shall not, in any way, be disclosed by a bank.”</td>
</tr>
<tr>
<td><strong>South Korea:</strong> The Act on Promotion of Information and Communication Network Utilization and Information Protection of 2001 protects the personal information of consumers held by certain industries. The number of industries subject to this law is in the process of being greatly expanded by the responsible government ministry.</td>
</tr>
<tr>
<td><strong>Taiwan:</strong> The Computer-Processed Personal Data Protection Law of 1995 protects the processing of personal data in certain kinds of industries, such as financial. It allows for restrictions on cross-border transfer of personal information.</td>
</tr>
</tbody>
</table>

In **Malaysia**, the **Philippines** and **Thailand**, new privacy legislation is expected to be enacted soon, while in **Indonesia** and **Vietnam** the e-transactions laws include privacy provisions. **New Zealand** is currently considering amendments to the Privacy Act of 1993 to protect cross-border movement of data and align its rules with the EU’s data protection regimen.
**ESI considerations**

When addressing the issue of whether to compel a party to produce data for pre-trial discovery, a court may consider additional factors solely related to ESI. There are a number of characteristics of ESI that are different than paper documents. These include:

- volume and ease of replication;
- persistence;
- dynamic nature;
- existence of hidden metadata;
- hardware and software system dependence and obsolescence;
- mobility, portability and searchability.

In *Aerospatiale*, the Supreme Court stated that the individual courts should show “special vigilance to protect foreign litigants from… unduly burdensome discovery” and specifically noted that courts must watch out for discovery abuses for overseas litigants based on “additional costs” and special problems on account of the “location of its operations.”

The FRCP allows a responding party to resist discovery of ESI that is not reasonably accessible due to undue burden or cost. The requesting party then has to show good cause to go forward with obtaining discovery, at which point the court will analyze the following additional factors, some of which are similar to those in the comity analysis:

- the specificity of the discovery request;
- the quantity of information available from other and more easily accessed sources;
- the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
- predictions as to the importance and usefulness of further information;
- the importance of the issues at stake in the litigation;
- the parties’ resources.

In addition to these factors, a court may also shift the cost burden of production to the requesting party. The Sedona Conference has documented a list of 12 factors to determine the relative accessibility of a source of potentially discoverable ESI. Six factors are based on media type (from *Zubalake I*) and six are based on data complexity. While none of these factors specifically relates to overseas ESI, the need for language translation from a local (possible...
Thank you to the IAPP members and friends who contributed their time and expertise to *The Privacy Advisor* this year. The IAPP and *Privacy Advisor* readers appreciate your commitment to sharing knowledge and advancing the privacy profession.

Martin Abrams  
Shannon Ballard, CIPP, CIPP/G  
Matthew Barach  
Jillian Barber  
Teresa Basile  
Jean-David Behlow  
Steven Bennett  
Ann Bevitt  
Lars Brauer  
Joshua Briones  
Ann Cavoukian  
Daniel Cooper  
Chris Cowper  
Malcolm Crompton, CIPP  
Richard Cumbley  
Lothar Determann  
Jan Dhont  
Larry Dobrow  
Erin Egan  
Debra Farber, CIPP, CIPP/G  
Julie Ferguson  
David Fink  
D. Reed Freeman Jr., CIPP  
Stephen Gantz, CIPP/G  
Pascale Gelly  
Craig Gentry  
Kirk Herath, CIPP, CIPP/G  
Rebecca Herold, CIPP  
John Jager, CIPP/C  
Jacqueline Kosek, CIPP  
John Kropf, CIPP, CIPP/G  
Christopher Kuner  
Sagi Leizerov, CIPP  
KX Lim  
Annie Lindstrom  
Marc Leeuwenthal, CIPP  
David Loukidelis  
Christine Lyon, CIPP  
Joanne McNabb, CIPP, CIPP/G  
Terry McQuay, CIPP, CIPP/C  
Flemming Moos  
David Morgan, CIPP, CIPP/C  
Kirk Nahra, CIPP  
Brian O’Connor, CIPP  
Dan Or-Hof, CIPP  
Tom Oscherwitz, CIPP  
Hamlet Pearson, CIPP  
Jose-Luis Pinar Manas  
Jules Polonetsky, CIPP  
Larry Ponemon, CIPP  
Michael Power  
Olivier Proust  
Nick Puji  
Richard Purcell, CIPP  
Elisabeth Quillatre  
Jorge Rey  
Christoph Rittweger  
Stewart Room  
Lauren Saadat, CIPP, CIPP/G  
Janelle Sahouria  
Luis Salazar, CIPP  
Heidi Salow, CIPP  
Bruce Schneier  
Mathew Schwartz  
Andrew Serwin  
Thomas Shaw, CIPP  
Julie Sinor, CIPP  
Daniel Solove  
Lisa Sotto  
Mike Spinney, CIPP  
Jennifer Stoddart  
Zoe Strickland, CIPP, CIPP/G  
Anaht Tagvoryan  
Florian Thoma  
Micah Thorner  
HenrietteTelemans  
Eduardo Ustaran  
Tanguy van Overstraeten  
Richard van Staden ten Brink, CIPP  
Jarno J. Vanto  
Maria Villar  
Christopher Wolf  
Amy Yates, CIPP  
Jonathan Zittrain
BELGIUM

By Jan Dhont

‘Dear valued customer, we regret to inform you that your data has been compromised...’

Paving the way for new standards in data security, on October 26, 2009, the Council of the European Union approved the directive amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the Directive). Following a trend, these amendments introduce notification requirements on public providers of electronic communication services in the event of data breaches. Such notification requirements exist in the U.S. and have been recently implemented in Germany, with many other European nations soon to follow.

Under the amended Directive, providers of publicly available e-communications must notify the relevant national authorities without delay when a personal data breach has occurred. A data breach is vaguely defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to” personal data.

Providers must also notify individuals or subscribers of electronic communication services if the breach is likely to adversely affect their personal data or privacy. Notification to a customer or subscriber will not be required if the provider can demonstrate that it has implemented certain protection measures to the satisfaction of the competent national authorities.

Further, the national authorities are granted the right to require notification regardless of the harm to the individual. Notifications should contain the nature of the breach, contact information and possible steps to mitigate damages and, if to the national authorities, the consequences and measures taken by the provider to address the breach. Additionally, national authorities are authorized to adopt guidelines on the notification process and are empowered to audit the service providers’ compliance. The providers are required to keep a log of breaches and any mitigating steps taken.

Following notification trends in the U.S., healthcare, insurance, and financial services industries will likely be the next industries affected by notification requirements. The European Data Protection Supervisor stated that “citizens will expect such a system to apply not only to their Internet access providers, but also to their online banks and online pharmacies” (EDPS press release January 12, 2009). The amendment recitals state that all EU member states should implement mandatory notifications for security breaches in all industries “as a matter of priority” and that a subsequent review on the member’s legislation in this respect, the Commission should take steps to encourage notification laws throughout the EU, “regardless of the sector, or the type of data concerned.” Thus, it is anticipated that notifications will branch out into other industries throughout Member States.

Overall, companies should consider their data security policies and procedures and assess their implementation of IT risk management in light of the new notification requirements. This is especially attenuated with regard to assessment of risks and harm to individuals and communication channels with the relevant national authorities.

Global Privacy Dispatches

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

CANADA

By John Jager, CIPP/C

Disclosure of subscriber information by Internet service providers

A number of recent court decisions have discussed the matter of Internet service providers (ISPs) providing law enforcement with subscriber information (SI) absent a court-issued warrant or subpoena.

In the most recent case dealing with this matter, the Ontario Court of Justice, in Her Majesty the Queen and Douglas Cuttell, found that the defendant had a reasonable expectation of privacy in his SI and that a warrantless request by police to the ISP for the defendant’s SI was a violation of section 8 of the Charter of Rights and Freedoms. In this case, the police came across the defendant’s IP address during an investigation of child sexual exploitation and requested that the ISP provided the subscriber’s SI, which it did in line with its policy. The ISP had developed a protocol to provide law enforcement agencies with SI without a warrant or subpoena only in the case where that information was requested by the police in the context of a child sexual exploitation investigation. All other disclosures of SI, for example for a fraud investigation, would not be made absent a
The court ruled that, in this case, the evidence obtained by means of a search conducted of the defendant’s home under a search warrant obtained on the basis of the defendant’s SI received from the ISP would be permitted, as society’s best interests were served by the admission of this evidence.

In its reasons, the court noted that sections 7(3)(c) and 7(3)(c.1) of the Personal Information Protection and Electronic Documents Act (PIPEDA) provide for a number of disclosures without consent of the individual. Although the police relied on section 7(3)(c) as its authority for making the request, the court pointed out that this section does not create a police ‘search power,’ it merely requires that a lawful authority exist before the personal information is disclosed without knowledge or consent. As such, it does not itself confer the authority to the law enforcement agency. The court also explored the role of the ISP’s privacy notice and other agreements between the ISP and the subscriber. The court cited a number of cases where it was found that as a result of a contract between the ISP and the subscriber, there was no reasonable expectation of privacy in SI (see, among others, R. v. Wilson, R. v. Ward, and R. v. McGarvie). In this case, however, the ISP could not provide evidence of what was posted on the company’s Web site or what was provided to customers at the time the defendant became a subscriber. The court noted that ISPs recognize a degree of privacy in SI, but that many ISPs have contracts in place that require subscribers to agree to disclosure of SI in certain circumstances and that therefore, in most cases, the issue of whether there is an expectation of privacy in SI will be resolved by the contract between the parties.

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

---

**FRANCE**

*By Pascale Gelly*

**Data sharing: disclosure of partners required**

In an answer to a query brought by the online magazine PCimpact.com, the CNIL (the French data protection authority) clarified what should be considered “informed consent” (opt in). In cases where a business intends to share personal data with other business partners, the individuals concerned should be put in a position to identify all data recipients. “The list should be up to date at the time the Internet user’s consent is collected and the Internet user should, as the case may be, be informed on the data collection form (or on the partners list if it is linked via a hyperlink) of the fact that the list may evolve.”


**E-discovery**

The CNIL issued a recommendation to data controllers requested to transfer information to the U.S. in the framework of e-discovery proceedings. French legal requirements must be met including those resulting from the Hague Convention and from the Data Protection Act.

**10 security recommendations**

The security requirements of the French Data Protection Act being expressed in general terms, the CNIL recently issued 10 recommendations to guide IT and security managers, including:

- creating a robust password policy (personal, confidential, of at least eight alphanumeric characters, renewed

See, Global Privacy Dispatches, page 12

---

**Privacy Classifieds**

*The Privacy Advisor* is an excellent resource for privacy professionals researching career opportunities. For more information on a specific position, or to view all the listings, visit the IAPP’s Web site, www.privacyassociation.org.

**PRIVACY ANALYST**

Zions Bancorporation
Houston, TX

**PRIVACY ATTORNEY**

Wells Fargo
Charlotte, Des Moines, Minneapolis, or San Francisco

**PRIVACY COMPLIANCE SENIOR ASSOCIATE**

Freddie Mac
McLean, VA

**PRIVACY MANAGER**

Prescription Solutions
Irvine, CA

**SENIOR SECURITY & IDENTITY SERVICES ANALYST**

Legacy Health
Portland, OR

**PRIVACY CONSULTANT**

Convergys
Cincinnati, OH

**CHIEF INFORMATION SECURITY OFFICER**

Wright Express Enterprise
South Portland, ME

**DATA SHARING CONSULTANT**

Axiom
Falls Church, VA

**MANAGER, PRIVACY & GOVERNMENT AFFAIRS**

The McGraw-Hill Companies
Washington, DC

**SENIOR COUNSEL, PRIVACY AND REGULATORY MATTERS**

Omnichannel Media Group
New York, NY
**Global Privacy Dispatches**

continued from page 11

every three months, that’s a robust password!);  
• managing user accounts, which should be personal as opposed to generic;  
• securing work stations with automatic screen saver;  
• creating a strict definition of user access depending on user profile based on need to know;  
• ensuring data confidentiality by service providers beyond mere contract clauses;  
• securing local networks (logical protection, specific caution for remote access by portable devices…);  
• securing premises: access control, badges;  
• anticipating the loss or disclosure of data: regular backups, emergency recovery process, specific protection of portable devices (encryption) depending on content sensitivity;  
• anticipating and formalizing an IS security policy;  
• user sensitization to IT risks and to the Data Protection Act.

**“Peer to peer law” — the status**  
As reported in the October issue of the Privacy Advisor (page 10), the law to fight against infringing downloads had to be modified in order to meet the requirements of the French Constitutional Court. Finding the new draft still unsatisfactory, some MEPs challenged it once more before the Constitutional Court. This time, the Court approved most of the text.

The principle of “graduated risposte” was maintained:

• Rightful owners can report an unlawful download to a High Authority, which will identify the Internet subscribers with the assistance of Internet access providers, and send them two warnings.  
• In case of repetition, a summary criminal procedure can be launched without trial; the sanctions being fines and the suspension of the Internet access.

The Ministry of Culture announced members of the High Authority in November and the first e-mail warnings will be sent at the beginning of 2010.

**Video-surveillance sanctioned**  
The CNIL issued a 10,000 euro fine to a street-ware business for using a permanent video surveillance system. The system, intended to protect the business against theft, was found not proportionate because it surveilled too many areas, including areas where no products were stored. The matter went before the criminal jurisdiction because the business manager had prevented the CNIL from conducting an onsite investigation. He was personally fined 5,000 euros by the Court.

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

**UK**

By Eduardo Ustaran

**UK government consults on tough penalties for the misuse of personal data**

The UK Government has launched a public consultation on whether to introduce prison sentences for those found guilty of offences related to obtaining, disclosing, or selling personal data.

The consultation paper “Knowing or Reckless Misuse of Personal Data: Introducing Custodial Sentences” proposes increasing the current maximum penalty from a fine to up to two years’ imprisonment. The proposed new measure could see those convicted imprisoned for up to two years if the case is heard in the Crown Court, and up to 12 months if heard in the magistrates’ court. The courts will also be able to impose community sentences and fines if appropriate.

The consultation will also look at whether a defence should be introduced for those acting for the purposes of journalism, art, or literature with a view to publishing such material in the reasonable belief that the obtaining, disclosing, or selling of the information is in the public interest.

**Consumer watchdog scrutinises customised pricing based on online behaviour**

The Office of Fair Trading (OFT) has launched two separate market studies into advertising and pricing. The first, into online targeting of advertising and prices, will cover behavioural advertising and customised pricing, where prices are individually tailored using information collected about a consumer’s Internet use. It is expected that this study will be completed by the spring of 2010. The second, into advertising of prices, will consider various pricing practices which may potentially mislead consumers. The study will look in particular, but not exclusively, at how these practices are used online. The OFT is reported to be increasingly concerned about how information about consumers’ Web usage is being surreptitiously exploited and the lack of control by consumers over their online personal data.

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

How many fax machines and printers are in your office?

Who makes the decision on how sensitive printed documents are disposed? Do you really know?

**THE SHREDDERS** specializes in securely disposing of sensitive material. The Shredders’ employees (Two guards per vehicle) that pick up and shred your material to confetti size particles are fingerprinted, DOJ background checked State Licensed Security Guards.

Most all shredding companies use the “Strip shredding or the Pierce and tear process”. These methods have flaws...you can read information on the strip and it could be put back together. Current laws state that “shredded material must be rendered unreadable”. Ask your current service provider to show you the shredded pieces then call us to get the job done right! Don’t risk your company’s or customer’s security by using an on-site shredding service!

“Today there is software that allows for reconstruction of shredded material.”

The Shredders modern fleet serving California from San Diego to Fresno!

For more information please visit [www.theshredders.com](http://www.theshredders.com) or if you would like a tour of our facility please call 800-222-2044 and we will be happy to show you the difference.
Congratulations, Certified Professionals!

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

Kevin Acoveno, CIPP/G
Kimberly Joy Akre, CIPP
Rami A. Albalawi, CIPP
Gregory Albertyn, CIPP
Miranda Alfonso-Williams, CIPP/IT
Michael Christian Bell, CIPP/IT
Adam T. Berg, CIPP
Astra Verdun Bester, CIPP/IT
Taryn Bevilacqua, CIPP
José A. Bisbe, CIPP
Andrea Blander, CIPP
Carlos M. Bonet, CIPP
Vicki L. Bowman, CIPP/G
Diane G. Boyea, CIPP/G
Gary Mark Brown, CIPP
Sarah Buerger, CIPP/IT
Merlene Burnham, CIPP/G
Kimberley Anne Bustin, CIPP/C
Katherine A. Careno, CIPP
Sheila R. Caudle, CIPP
Mary Elizabeth Cavanaugh, CIPP
Christopher T. Chihi, CIPP/G
Kate Gordon Cohen, CIPP
Kenneth Comstock, CIPP/IT
Keith P. Cooley, CIPP/IT
Lazaro F. Corrales, CIPP/IT
Ruth Day, CIPP
Barbara S. Dassenbrock, CIPP/G
Frank Robertson Dawson, CIPP/IT
Dennis Brian Dayman, CIPP
Thomas J. De Deo, CIPP
Russell Ray Densmore, CIPP/IT
Sunita Deshmukh, CIPP
Mark Arthur Di Sabato, CIPP/IT
Russell E. Dougherty, CIPP
Ron N. Dreben, CIPP
Neil Alexander Etter, CIPP/G
Elizabeth Ann Fearnlow, CIPP
Caitlin Davitt Fennessy, CIPP
Donna H. Fickert, CIPP/G
Katherine Ann Fileherty, CIPP
Jonathan Fox, CIPP
Linda Gaye Fumey, CIPP
Sarah Gagwani, CIPP/IT
Glen Alan Germanowski, CIPP
Susan M. Gifaldi, CIPP
Joanna Lyn Grama, CIPP/IT
Natalie Tull Greene, CIPP
Teresa Elizabeth Hall, CIPP/IT
Daniel John Heinle, CIPP/IT
William Keith Horstman, CIPP/IT
Daniel M. Hoye, CIPP
Catherine Intravia, CIPP
Trina L. Jackson-Ford, CIPP/IT
Ronney Alex John, CIPP
Richard Allen Johnson, CIPP/G
Gina Julian, CIPP/G
Lew A. Kaufman, CIPP/IT
Yvette D. Kelly, CIPP/G
Michael Fergus LaMothe, CIPP/G
Scott K. Larron, CIPP
Michelle Diane Levack, CIPP/G
Chad Oliver Lewis, CIPP/G
David A. Lowe, CIPP/G
Joseph Patrick Lynem, CIPP/G
Mita Majethia, CIPP/G
Michael Joseph Marshall, CIPP
John Scott Mathews, CIPP
Mark Jason Molloy, CIPP/G
Sarah D. Morrow, CIPP
Susan K. Moscaritolo, CIPP
Erin Jeannette Mount, CIPP/IT
Mra Khwar Nyo, CIPP
Kingsley Odeh, CIPP
Robert A. O'Keefe, CIPP
Joseph Dennis O’Leska, CIPP/G
Patrick O’Malley, CIPP
Genevieve Marie Ovall, CIPP
Steven William Owen, CIPP/G
Michael Owings, CIPP
Geoff Palmer, CIPP/G
Erick Rowlind Patterson, CIPP/G
Robert S. Perdue, Jr., CIPP
Camille D. Privett, CIPP/G
Peggy Lyn Pugh, CIPP/G
Robert B. Quigley, CIPP
Vicki Shaw, CIPP/G
Robert S. Ricketts, CIPP
David Andrew Ritchie, CIPP
Perry Christian Robinson, CIPP
Melissa J. Rolf, CIPP
Andrew P. Sargent, CIPP
James Watson Schreiber, CIPP/G
Thomas Mark Scarrah, CIPP
Vickie Shaw, CIPP/G
Daniel J. Showalter, CIPP/IT
Jack Showalter, CIPP/G
Marie A. Simonelli, CIPP
Susan Smith, CIPP
Christopher Strobel, CIPP
Brendan Paul Sweeney, CIPP/IT
Peter Brian Tannish, CIPP
Chad R. Thiemann, CIPP
Aubrey Craig Turner, CIPP
B. Diane Ury, CIPP/G
Bernardo Manuel Vasquez, CIPP
Scott John VonFischer, CIPP/IT
Kathleen Anne Wakefield, CIPP/IT
John J. Walker, CIPP/G
Joann E. Waters, CIPP/G
David J. White, CIPP
Joshua Jon Wieland, CIPP/IT
Susan K. Williams, CIPP
Amadou Yattassaye, CIPP/IT
Linda Dawn Zanfardino, CIPP
Patrick Edward Zeller, CIPP

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

If you are a recent CIPP, CIPP/G or CIPP/IT graduate but do not see your name listed above then you can expect to be listed in a future issue of the Advisor. Thank you for participating in IAPP privacy certification!
Reidenberg was not stalking the Justice. Rather, he launched the educational exercise in response to the assertion by Justice Scalia at a privacy conference in January that he didn’t think “every single datum about my life is private.” (The dossier the Fordham students prepared never was released to the public.)

The Justice was furious, calling the class exercise in Googling a demonstration of bad judgment. Analogizing to the First Amendment, the Justice said that just because the law allows you to do something does not mean you should do it.

At a recent IBM-sponsored program, the issue of privacy and ethics was discussed, with a particular focus on the episode of Scalia Googling. One aspect of the issue was whether, in the Google/MySpace/YouTube era, anyone—even a public figure—can have an expectation of privacy when it comes to publicly available information that appears online. For sure, information provided in private, or for one particular purpose, is ending up on the Internet for all to see. Does that mean there should be a rule of ethics that even though information is publicly available, one should refrain from looking at it (or downloading it)?

The rules on intellectual property are a lot clearer: Just because copyrighted sound recordings and motion pictures may be available for download on the Internet does not mean we should take them for free. It’s illegal. But there are no legal rules on helping ourselves to freely viewable personal information online. That, as Justice Scalia has put it, is a matter of “judgment.”

To be sure, there are legal restrictions on what personal information can be accessed from credit bureaus and for what purpose it can be used. And other companies that provide personal information to law enforcement and business operate under legal rules. But for the great maw of information available online, it is pretty much “anything goes.”

In his book, Delete: The Virtue of Forgetting in the Digital Age, Viktor Mayer-Schönberger explains that forgetting is a natural human process, but that digital technology and cheap storage make forgetting impossible. So we appear to be approaching the fictional world of the movie Defending Your Life with Albert Brooks and Meryl Streep, in which anything goes.

See, Ethics of Googling, page 24
WORKSHOP SESSIONS OFFERED:
A week’s worth of privacy education, with sessions such as...

- Online Privacy: Behavioral Targeting and Beyond
- Cloud Computing: Demystifying the Issues and Managing the Risk
- Global Transfer Solutions: Selecting a Solution That Works for Your Organization
- Privacy and Corporate Responsibility
- Protecting the Privacy of Minors
- Balance between Privacy and Security
- Companies, privacy and international data flows
- Intellectual property and privacy: profiles of a conflict
- Data protection law in a globalized world
- New advertising techniques and privacy
- Do you have a private life at work?
- Privacy by Design
- Towards a global regulation on privacy: proposals and strategies
On Tuesday, the IAPP held its Data Protection and Privacy Workshop at the Melia Castilla hotel. In this session, privacy experts from four continents discussed “The Future of the Privacy Profession.” (LtoR) Bruno Rasle, French Association of Data Protection Correspondents; Maria Belen Cardona of the Spanish Association of Privacy Professionals; Christoph Klug of the German Association for Data Protection and Data Security; Malcolm Crompton, IAPP/ANZ; Kamlesh Bajaj, Data Security Council of India; David Hoffman, Intel; Bojana Bellamy (moderator), Accenture.

Ontario, Canada Information and Privacy Commissioner Ann Cavoukian at her event, Privacy by Design: The Definitive Workshop, which she co-hosted with Yoram Hacohen, head of the Israeli Law, Information, and Technology Authority.

Privacy and corporate responsibility was the focus of this panel. (LtoR) Willemien Bax, European Consumers’ Organization (BEUC); Martin Abrams, Centre for Information Policy Leadership, Hunton & Williams; Bojana Bellamy, Accenture; New Zealand Privacy Commissioner Marie Shroff (moderator); Fran Maier, TRUSTe.

Leslie Harris of the CDT makes a point during lunch at the IAPP Data Protection and Privacy Workshop.

The 32nd International Conference of Data Protection and Privacy Commissioners will take place in Jerusalem, next October.
bly double-byte) language into English or additional legal reviews for confidentiality and relevance of foreign language ESI performed by foreign-qualified attorneys may provide the basis for an undue burden or cost argument.

Conversely, the third factor from the Restatement’s comity analysis discussed above (“whether the information originated in the U.S.”) could be used to support an argument for discovery of ESI that may have originated in the U.S. but was then moved overseas. This may be quite typical in the emerging cloud computing environment.

Finally, local e-discovery rules are being introduced, such as Australia’s Practice Note 17 or Singapore’s Practice Direction No. 3, and their effect on U.S. courts’ analyses of overseas ESI discovery is yet to be determined.

**Conclusion**

Asia-Pacific parent corporations with U.S. subsidiaries or operations should, as a first step, perform a proactive legal risk analysis for their exposure to U.S. pre-trial discovery based on the factors outlined in this article. As a second step, these non-U.S. parent corporations should analyze how prepared they currently are to respond in a timely manner to pre-trial discovery requests. This would include performing at least an inventory of the corporate data and data custodians, analyzing records retention and legal hold processes to guard against improper deletion of responsive data, and verifying that data collection procedures are legally sound. As a third step, all remediations identified in the first two steps should be designed, implemented, and monitored. It is critical that these companies enlist the proper expertise to help them through this multi-disciplinary process, including technically adroit attorneys who understand the international legal analysis required and IT resources with detailed knowledge of both the corporate data and the numerous processes needed to identify, preserve, collect, process, review, and produce data responsive to U.S. litigation.

Part one of this series can be found in the November issue of the Privacy Advisor, available online at www.privacyassociation.org (click “educate,” then “Advisor archives”).

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

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

Subscribe to our Privacy Law Blog at
http://privacylaw.proskauer.com/index.xml
**eBay receives BCR approval**

Ebay has received permission to use binding corporate rules (BCRs) to transfer data across borders. The Luxembourg data protection authority, Commission Nationale pour la Protection des Données (CNPD), approved the company’s application recently.

BCRs are legally binding regulations that demonstrate a company’s capacity to transfer data across borders safely. The approval lets eBay transfer and share personal data within the company without having to use other legal instruments such as model contractual clauses.

“We were very pleased with the exceptional work provided by [eBay and eBay’s outside counsel Allen & Overy], of the quality of the documents elaborated and of the constructive dialogue in the process of validation and implementation of eBay’s binding corporate rules,” said CNPD President Gerard Lommel.

eBay is the first e-commerce company to receive BCR approval, according to a company press release. It gained approval for both employee and customer BCRs. The authorization came under the new BCR mutual recognition procedure.

EBay Global Privacy Leader Scott Shipman, CIPP, called the approval a “major milestone” and said: “The level of cooperation and communication eBay received from the CNPD and the other DPAs was greatly appreciated and made the project a success.”

**Breach action site created**

A new site aims to provide a one-stop resource for organizations that have experienced a data breach. Field Fisher Waterhouse (FFW), RSA Security, and KPMG have teamed together to create the Breach Action Web site, a clearinghouse of law, technology, and consultancy resources who will collectively execute a joint plan of action for breached firms.

“The Breach Action Web site was devised to provide speedy access to relevant experts should the worst happen,” said FFW Privacy & Information Law partner Stewart Room. “By offering this holistic service we hope that companies suffering a data breach will be able to minimize the impact of the breach and its consequences.”

www.breachaction.co.uk

**Walters joins U.S. SEC as FOI/Privacy Act chief**

Barry Walters is the new chief Freedom of Information Act and Privacy Act officer at the Securities and Exchange Commission.

“I am pleased to welcome Barry back to the SEC,” said the commission’s general counsel and senior policy director, David Becker. “Given the great importance of making sure investors receive the information they need, and handling sensitive information in a secure manner, I am confident his experience in these areas will serve the agency well.”

Walters served as FOIA/Privacy Act Officer at the SEC from 2001-2002, according to an SEC press release. He returns to government after several years in the private sector.

“It is a pleasure for me to return to the commission to serve in this important position,” Walters said.

---

**New AFCDP board members**

The French Association of Data Protection Correspondents (AFCDP) has named new members to its board of directors.

New board members include correspondants information et libertés (CILs) Patrick Blum of Essec; Laurent Cellier of Deveryware; Dominique Chaumet of RATP; Marc Dolo of Casino; Pascale Gelly of Cabinet Gelly; Helene Legras of Areva; Catherine Leverrier of Groupama; and Herve Josse of La Poste.

Denis Beautier of ISEP and Jean-Pierre Remy of Banque de France were re-elected to the board, as were AFCDP executive officers.

AFCDP was created in 2004 after the Data Protection Act was amended to create the function of the data protection correspondent. It is a forum for privacy and data protection professionals and others who are interested in the protection of personal data.

The new board says it will begin working on an ambitious four-year development plan which will include workshops, regular meetings, and the creation of guidance documents, among other initiatives.
Engaging data

More than 200 people from across the globe attended the First International Forum on the Application and Management of Personal Electronic Information in October, the launching event of the MIT SENSEable City Lab’s “Engaging Data Initiative.”

The Engaging Data Initiative seeks to address the issues surrounding the application and management of personal electronic information by bringing together the main stakeholders from multiple disciplines, including social scientists, engineers, manufacturers, telecommunications service providers, Internet companies, credit companies and banks, privacy officers, lawyers, watchdogs, and government officials.

The forum explored novel applications for electronic data and addressed the risks, concerns, and consumer opinions associated with the use of this data. Participants discussed techniques and standards for protecting and extracting value from this information.

— Caitlin Zacharias

The Privacy Projects

New initiative to fund ‘evidence-based’ privacy research

A new nonprofit research institute has been created to fund academic research about privacy. The Privacy Projects will forward research intended to help maintain the balance between the use and protection of personal data.

“Technology and consumer demand for Internet-based services have clearly outpaced many of the laws and regulations initially put in place to protect consumers,” said TPP President Richard Purcell, CIPP. “Our goal is to provide evidence-based information to support the dialogue toward establishing increased corporate accountability and greater regulatory relevance to today’s information economy.”

The Privacy Projects released its first research paper at an event in Paris recently.

www.theprivacyprojects.org

Calendar of Events

JANUARY 2010

28 Data Privacy Day
Locations worldwide
www.dataprivacyday2010.org

28 FTC Privacy Roundtable
University of California
Berkeley School of Law
Berkeley, CA

28 Privacy by Design: The Gold Standard
Toronto, Ontario
www.privacybydesign.ca

28 Privacy After Hours
Locations worldwide
www.privacyassociation.org

FEBRUARY

4 Université AFCDP des Correspondants Informatique & Libertés
Paris, France
www.afcdp.net

MARCH

16 IAPP Tenth Anniversary Celebration
www.privacyassociation.org

17 FTC Privacy Roundtable
FTC Conference Center
Washington, DC

APRIL

19-21 IAPP Global Privacy Summit
Washington, DC
www.privacysummit.org

MAY

26-28 IAPP Canada Privacy Symposium 2010
Toronto, ON

JUNE

14-15 Practical Privacy Series
Santa Clara, California

SEPTEMBER-OCTOBER

29-1 IAPP Privacy Academy
Baltimore, MD

To list your privacy event in The Privacy Advisor, e-mail Tracey Bentley at tracey@privacyassociation.org
In the Privacy Tracker this month...

If this month is any indication, the outlook for privacy in 2010 is red hot. Already in December:

- The Federal Data Accountability and Trust Act, HR 2221 (Rush, D), passed the House and moved to the Senate. The bill requires data security policies and procedures and provides for nationwide notice in the event of a security breach.

- S 1490 (Leahy, D), which also requires a comprehensive data security program by businesses that maintain personally identifying information, passed out of the Senate Judiciary Committee.

- The FTC held its first of three privacy-focused roundtables, where issues surrounding online and mobile advertising received considerable focus.

Don’t miss easy-to-read weekly and monthly updates on the privacy legislation you need to know about. The Privacy Tracker will keep you up-to-date on all 2010 federal and state privacy legislation, with monthly audio conferences (where you can request specific coverage), weekly e-mails, and a Web dashboard featuring timely articles and reports.

Subscribe today to keep up with the privacy developments affecting your business.

Try it before you buy it! E-mail us to get a free week-long demo subscription to the Privacy Tracker.

www.privacytracker.org

Did You Know?

Pandemic privacy
The offices of the privacy commissioners of Canada, British Columbia, and Alberta have released guidance about how privacy laws apply in the private sector workplace during the H1N1 pandemic.

www.privcom.gc.ca

Wanting more
In a recent survey, 71 percent of UK employees indicated that their organizations should do more to protect confidential documents. The numbers were similar among employees in other European nations: Germany (66%), Belgium (70%), Netherlands (61%), Ireland (85%).

Source: National Fraud Authority

Data matching
The Office of the Privacy Commissioner of Victoria, Australia, has published guidance on data matching. The guidance is targeted to the public sector, but private entities such as financial institutions and advertisers may also find it useful.

www.privacy.vic.gov.au

The Lighter Side of Privacy

Reprinted with permission from Slane Cartoons Limited.
What do you know?

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

What's next for your business?
ey.com/privacy
Ethics of Googling continued from page 15

which every episode in one’s life is recorded for later viewing (to pass judgments).

As much as Justice Scalia would like, it is unlikely that society will develop ethical norms about accessing freely available online personal information. So should we just throw up our hands and conclude in the words of former Sun Microsystems Chairman Scott McNealy that “there is no privacy, get over it”? Actually, privacy is both a matter of giving and taking. Yes, personal information online is free for the taking and that is not likely to change. But we still have lots of ability to control what personal information is taken from us, and for what purpose—the personal information that has the potential to end up online for public view. The legal and ethical problem so far has been on how we are informed about who is taking our information, for what purpose, with whom it is being shared, how long it will be retained and when (and how) it will ultimately be destroyed.

The Federal Trade Commission has gotten a lot tougher recently about the notices that companies give about the collection of online information, and new FTC leadership is focusing hard on that question. Congressman Rick Boucher is proposing new legislation to control online tracking of consumers for targeted advertising. And many think that our “digital natives,” the kids who have grown up with computers and social networking sites, need to be educated about the permanent record that the online world creates. Funny pictures from a fraternity bash or an irreverent “tweet” on Twitter may impede a young person’s educational or job opportunities.

Responsible companies, too, are recognizing, as a matter of law and business ethics, that providing clear and timely notice to consumers about the collection and use of information from them builds trust. In this age where information is the lubricant of commerce, being fair to people about their personal information is not just the right thing to do, it is good business. The Future of Privacy Forum, a think tank focused on privacy issues, is working on new ways online marketers can engage users about how their Web activity is being used for tailored advertising.

So, we may never solve the problem of all of us becoming online voyeurs, accessing and looking at personal information about others because we can. “Googling someone” has entered common parlance precisely because it is common. But as technologies accelerate in their ability to collect information about us, providing each of us with control on the input side of things is imperative.

Mr. Wolf leads the privacy law practice at Hogan & Hartson LLP and is the co-chair of a think tank focused on privacy issues, the Future of Privacy Forum. This article is an adaptation of a recent presentation at the IBM IT Services Legal Summit in New York City.