Genomic pioneers blaze trail to new frontier

By Annie Lindstrom

Would you share your genomic information with the world at large via the Internet? That’s a question ten people had to answer before taking part in a Harvard Medical School project that will do just that. Annie Lindstrom speaks with participants in the Personal Genome Project.

The PGP-10 is a small group of ten pioneers who are taking the phrase, “I’m an open book” and the science of genetics to a whole new level. They are the first of what Harvard Medical School hopes will be an eventual 1,000 people who will be willing to forsake privacy concerns and share their genomic information, DNA sequences, medical records, and other personal information with the research community and the general public as part of a study called the Personal Genome Project (PGP).

The study follows in the footsteps of the Human Genome Project (HGP), which in 2001 provided the first drafts of nearly complete human genome sequences. Such information has since been used to advance medicine, human biology, and knowledge of human origins. George Church—an HGP initiator, director of the PGP and one of the PGP-10, himself—hopes the PGP-10, and the 1,000 people to come, will spark the general public’s interest in getting their own genomes sequenced.

See, Genomic pioneers, page 3

Europe debates mandatory data breach notifications

With the severity of data breaches on the rise, will Europe adopt U.S.-style mandatory disclosure of data privacy regulation violations?

By Mathew Schwartz

At the RSA Conference, IAPP London correspondent Mat Schwartz put an ear to the European debate on mandatory breach notifications. Here’s what he heard.

To notify, or not to notify?

Mandatory data breach notifications—public alerts whenever consumers’ personal information has been lost or stolen—are de rigueur in the United States. As a result, many companies have improved their data security safeguards and been forced to publicly apologize and compensate data-loss and identity theft victims.

See, Europe debates notifications, page 7
Guided by global voices

I write this only days after the annual Data Privacy Day. Data Privacy Day created a lot of buzz in this, its third year. Privacy regulators, governments, organizations, and businesses in 29 nations recognized the day in various ways. We were pleased to see so many IAPP members playing a big part in generating awareness about the important and challenging issues we work on every day.

The federal privacy commissioner of Canada, Jennifer Stoddart, perhaps put it best in her Data Privacy Day proclamation when she said that in today’s wired world, protecting and promoting privacy rights demands a coordinated approach. “This cannot be done on a province-by-province or country-by-country basis…,” she wrote. “The only way to achieve meaningful progress in such a complex environment is to work collectively to find broader solutions.”

Commissioner Stoddart and many other privacy regulators will join us next month in Washington, DC. Data protection authorities presenting at the Privacy Summit include Yann Padova, secretary general of the CNIL; Artemi Rallo, director of the Spanish Data Protection Agency; Yoram Hocohen, head of the Israeli Law Information and Technology Authority; Richard Thomas, UK information commissioner; Joanne McNabb, head of the California Office of Privacy Protection; and former privacy commissioner of Australia, Malcolm Crompton among others.

Where else can you interact with so many privacy regulators and the experts who help shape their policies?

We are also very excited to bring Frank Abagnale and Bruce Schneier to this year’s Summit. Frank Abagnale’s illustrious if brief career as an identity fraud extraordinaire makes him especially qualified to help fight identity crime, which is what he’s been doing for the last three decades. We look forward to Frank’s keynote address and breakout fraud seminar: “The Art of the Steal.”

Bruce Schneier previews his Summit keynote address in this issue of Privacy Advisor. See page 9 for more.

The IAPP Privacy Summit has become the largest and most global privacy event in the world. The area is growing, the issues are compounding, and this year’s event reflects that, with more than 60 educational and networking sessions from which to choose. We hope you will join us.

Sincerely,

J. Trevor Hughes, CIPP
Executive Director, IAPP
The more people who participate and share their information openly, the more geneticists and everyone involved will benefit, explains Church, who in addition to his role in the PGP is a professor of genetics at Harvard Medical School and a professor of health sciences and technology at Harvard and MIT.

One important factor that is likely to influence the general public’s interest in genomic sequencing is government assurance that their genetic information won’t be used to harm them. Earlier this year, Congress demonstrated its support of genomic exploration and associated commercial endeavors by passing the Genetic Information Nondiscrimination Act of 2008 (GINA). The Act alleviates some of the privacy and discriminatory concerns associated with collecting and sharing genomic information by prohibiting group health plans and insurers from denying coverage or charging higher premiums to a healthy individual who’s genome shows a predisposition for disease. GINA also prohibits employers from using genetic information to fire, or fail to hire or promote, an employee.

Nothing to hide

While GINA addressed some of their privacy concerns, the legislation was passed after most of the PGP-10 already had agreed to participate in the project. With or without GINAs protections, the PGP-10 had a lot to think about when making their decision to bare their personal information to the world. Privacy Advisor spoke with three members of the PGP-10—Misha Angrist, Esther Dyson and George Church—about what went into their decision to share their genetic and health histories with the world.

Misha Angrist
Assistant Professor, Duke University Institute for Genome Sciences & Policy

Angrist holds a doctorate in genetics from Case Western Reserve University and an MFA in writing from the Bennington writing Seminars. A former board-eligible genetic counselor, Angrist has worked as a researcher, biotechnology consultant, writer and editor. He is writing a book about personal genomics, which is one of several reasons he chose to join the PGP-10.

“Originally, I was just going to write a book about George Church, but when I found out about the PGP-10, I thought it would be more interesting to write about it from the inside. So, I put my name in the ring and was fortunate enough to be chosen,” says Angrist.

Secondly, Angrist says he’s “quite sympathetic” to Church’s up-front claim that keeping information of this nature private would be very difficult. Thirdly, Angrist says that if the goal of genomics is to understand what makes us human and how genes and environment impact one another, then anonymity “impoverishes” the data and limits the amount of knowledge that can be reaped from each participant and by the study as a whole.

Furthermore, the PGP encourages a more collaborative model for medical research as opposed to the guinea pig model that exists today in large part because of the need to keep study subjects’ privacy intact, he explains. Full disclosure, on the other hand, encourages and enables study subjects to be engaged in the process by providing their thoughts and information to those who are interested in them. Nevertheless, some precautions are in order, he adds.

“The PGP is looking for people who are inclined to give total access,” says Angrist. “I will probably put my data on the Web, but I want to look at it first. If I carry something scary then I want my children to find out from me and my wife.”

Angrist says that the ultimate purpose he and the rest of the PGP-10 serve by being involved in the project is their ability to “raise the possibility that genetic research can be viewed differently.”

“We don’t yet understand all the ways in which this information is, and will be, important, we hope we can publicize, demystify and destigmatize it.”

See, Genomic pioneers, page 4
Genomic pioneers
continued from page 3

Esther Dyson
Principal, EDventure Holdings

Board member and active investor in a variety of start-ups in the information technology, aviation/space travel, healthcare/genetics industries, Dyson’s approach to life and science is probably summed up best by the words that conclude her Web site bio—What I want on my epitaph: “I wasn’t done yet! There is still more to learn and to fix.” Among her many endeavors, Dyson also is a board member of 23andMe, a personal genomics company.

“I first heard about the PGP from George Church and I told him I would love to be part of it as soon as he got Independent Review Board approval,” says Dyson. “People think genetic information is so mysterious and powerful and scary. I wanted to help make people think that it’s really just some more information. Sometimes it’s interesting and sometimes it’s not.”

Learn more about genetics and privacy at the Privacy Summit next month.

SESSION:
Genetics Research and Privacy: Evolving Ethical, Legal and Social Implications

Hilary Wandall, CIPP, Attorney and Corporate Privacy Officer, Merck & Co.
Debra Bromson, Senior Counsel and U.S. Chief Privacy Officer, AstraZeneca Pharmaceuticals LP

Genetic/genomic research promises to revolutionize the practice of medicine and extensive resources have been devoted to exploiting the potential of genomics—including developing huge repositories of human biological samples for purposes of genotyping and other analyses. Bioethicists, however, have raised concerns about the privacy implications of “biobanking” and related genetics/genomics research. Our DNA not only can be used to identify us (i.e., our social identity), it IS us (in terms of our biological identity). And biological samples not only reveal information about us, they also reveal information about our family and ancestry. Explore the inherent privacy issues in genomic research and join the ongoing dialogue on the appropriate balancing of privacy interests with the broad social goal of advancing medical research.

“We rely on BNA’s Privacy & Security Law Report day in and day out. Its scope and depth of coverage is unparalleled. We get timely, accurate coverage with a balance that is not always easy to achieve in this area of law.”

Emilio W. Cividanes and Stuart P. Ingis
Partners, Venable LLP, Washington, DC

LEADING AUTHORITIES in e-commerce, privacy, data protection, marketing and information services law and policy.
AUTHORS & EDITORS of BNA’s forthcoming Corporate Practice Series Portfolio on privacy law.

www.bna.com
800-372-1033
Although she says she had no reservations about unveiling any health concerns that the project might reveal about her, either to herself or the world, she says she can understand that other people might have concerns and their own particular reasons for them.

"I’m not saying anyone should publish their information, I’m just saying it’s not crazy to do so," she says.

"The PGP will help improve general perception of genetic information as something useful rather than scary. And with luck, my information will be useful to someone," she adds. "What's really interesting isn't my genome itself, but the interpretation of the data and what it is likely to be correlated with. There's so much more we still have to learn and we need lots of genomes and associated health records to learn it."

Therefore, the more the merrier, says Dyson when asked about the general public diving into genome mapping.

"I think people should think it's a great idea, but they should be sensible and sensitive and make sure their family doesn't object. The more scientific information available the better," she says. "They can do it through the PGP and make it completely public, or they can contribute it privately through something like 23andMe, but sharing this information can actually be helpful to them as well as to lots of other people."

George Church
Director of the PGP and Professor of Genetics, Harvard Medical School, Professor of Health Sciences & Technology at Harvard and MIT

In 1984, Church co-developed the first direct genomic sequencing method and helped initiate the Human Genome Project. A host of scientific firsts later, he initiated the Personal Genome Project (PGP) in 2005. Church explains that his decision to become a participant in the PGP-10 was actually not his own idea.

"My Institutional Review Board thought I should experience the same risks and benefits as my research subjects," says Church.

Church says that when he started the PGP and research on human subjects, he was well aware of privacy concerns. He realized that the project would put a lot of data concerning identifiable genetics and traits in the same place.

"That was fairly rare then and is still quite rare. In fact, the PGP may be the only place both are together in an open access database," he adds. "I decided it would be better and safer for the project and the people involved to pick people that were well informed and that didn't care about anonymity."

While the study is in its beginning stages, data has been collected on all 10 participants. Each will be updated on their results along the way to their full genomic sequencing, he explains. However, money and resources will determine how much data is collected as the project proceeds.

"There is kind of a trade off between how much money and resources we spend per person vs. the total number of people who participate," says Church. "I'd prefer to have 100,000 people with less..."
Genomic pioneers

continued from page 5

than a full genome vs. a full genome on 1,000 people.”

Church adds that 8,000 volunteers are waiting in the wings to join in the study and that number will likely increase as scientific papers are released and people see exactly what’s going on, he adds.

Church says participating in the PGP is akin to a person donating their body to science before they die, but talk on the blogs he’s read is split between people who say participants are crazy because they will lose their insurance and those who say they feel sorry for people who can’t see beyond insurance concerns.

When he made his decision to join the PGP-10, Church says he had the same concerns as most people.

“Maybe not everybody cares about the project the way I do, but I thought through the insurance issues just the same,” says Church. “GINA was not in place when we started, but it’s in place now. It’s not perfect, but it’s an indication of where things are going, maybe.”

Church says the potential harms from learning about one’s genomic information include the possibility of a false-positive interpretation of their data. Potential risks of revealing one’s information to others could include people getting the impression or claiming that they know more about you than they actually do know, he explains.

As far as the benefits are concerned, Church says he doesn’t want to overstate them at this point.

“It’s definitely a team effort. The benefits to society are that if we all share our information, we will all get some benefits, he says. “Right away, benefits to the individual might be few. But, if you happen to have a debilitative disease with a cure, you could experience a huge benefit.”

As more software develops that can crunch the data and correlate it, participants could experience even more benefits, he adds.

“There are things that can happen when things are open that cannot happen when they are closed,” says Church.

“You can dream up ways you can accomplish things in a closed environment, but things can happen faster and in more open, integrated environments.”

As far as the average Joe is concerned, Church likens genomics today to computers in the 1970s. Back then, only geeks were interested in computers, he explains.

“Right now this is not essential for medicine, but I wouldn’t be surprised if five years from now everybody knows it,” says Church. “But until they know it, the average person should probably steer clear of it. But they can get to know what’s going on by looking at Web sites or the growing number and variety of resources.”

Annie Lindstrom is president of KittyHawk Communications, Cape Coral, Fla. Annie has worked as a freelance writer since 2000. Prior to launching her own business, she worked as a journalist for the telecommunications industry’s top trade publication since 1989.
Now, European Union officials are debating whether to make U.S.-style data breach notifications mandatory throughout the EU’s 27 member states, or even to go one better and impose civil penalties, including jail time, for violating data privacy statutes.

The ball got rolling in November 2007, when the European Commission (EC) suggested revising its “Directive on Privacy and Electronic Communications” (#2002-58) to include new security and data privacy requirements, including mandatory data breach notifications for “accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data.”

The only wrinkle: the directive applies solely to telecommunications companies and ISPs. Therefore the goal of the revision, says Anna Buchta, a policy officer for the EC, is to “harmonize” existing telecommunications and ISP laws and thus ensure an EU-wide “level playing field.”

The best consumer protection

But in this era of rampant data breaches, is such a narrow update what’s really needed? “Having it just for ISPs and telecoms providers? I’d say forget about it, it’s got comparatively little use to the consumer,” says Martha Bennett, research director for financial services at Datamonitor in London.

In fact, some EU agencies also want stronger medicine. The Council of Ministers, which fashions directives
together with the EC and the European Parliament, has argued for applying the revised directive to all entities handling private data. Likewise, the European Network and Information Security Agency (ENISA), which advises the EU on information security matters, recommends notifications for raising consumer, business and government awareness of today’s security shortcomings.

Buchta counters that the purpose of an EU directive is “to reflect only what is already in place in most member states” and thus “should be a quite high-level and general obligation which we hope would not lead to any conflicts with other security obligations.”

Five-legged sheep or harmony?

Will Europe find harmony through a proactive approach to data breach disclosure? Or will it settle for the lowest common denominator, producing legislation that Bennett says all too often resembles “the five-legged sheep with three tails?”

The progressive side of the fence includes the strict data protection laws of Germany and Scandanavia, where “opt-in” has been the dominant social principle for decades. And in Italy, which only recently passed a data privacy law, violators now face jail time.

Other countries, meanwhile, still have weak data privacy penalties. In the UK, for example, while public sector organizations must disclose data security incidents to the Information Commissioner’s Office (ICO), it can impose a maximum fine of only £5,000 ($7,400). “The Information Commissioner is about as efficient as a paper tiger,” notes Bennett.

And it shows: “I’ve regularly gone onto corporates and advised on security breaches which should never have happened: putting private data on test servers and making that live, leaking information onto Web sites in unsecured form, user data on memory sticks...” says Simon Briskman, a partner at London-based law firm Field Fisher Waterhouse LLP. “My message is that that hasn’t changed in the last 10 years or so. I was doing the exact same job in ’97 as in ’08.”

Giving UK enforcers some bite

Finally, after more than a year of embarrassing data breaches involving such agencies as the Ministry of Defense and HM Revenue & Customs, the government is increasing the ICO’s power to audit organizations and levy fines.
Schneier shares

Security expert expounds on heroism, Obama, and liberty versus control

Bruce Almighty is some other guy, but with Bruce Schneier’s cult-like following on Facebook and elsewhere, one might easily mistake the names. Here’s a preview of what you’ll hear when Bruce Schneier takes the stage at the Privacy Summit.

IAPP: You have a cult following on Facebook. One group is called Bruce Schneier for president (30 members); another calls itself Bruce Schneier is my hero (165 members). What is the most heroic thing you’ve ever done?

Schneier: I’ve never considered myself particularly heroic. What I think people are responding to is my ability to think clearly about, and explain, security systems—and to speak the truth as I see it, regardless of who it might piss off. Valuable, yes; but not heroism.

IAPP: Should Obama give up his BlackBerry?

Schneier: I have no idea. Security decisions always balance one thing against another. There are two major risks to President Obama keeping his BlackBerry. The first is illegal access: hackers, criminals, international intelligence agencies, and so on breaking into the BlackBerry network and gaining access to his communications. The second is legal access: subpoena, the Presidential Records Act, or the pressure of public opinion forcing him to make his communications public. Both are real risks. But Obama also receives benefits from having a BlackBerry—from having access to that type of communication. Only he can balance those benefits against the risks, and make a decision.

IAPP: Could too much privacy inhibit what we want to do with security?

Schneier: It’s a common misconception that security and privacy are opposites: that you have to give up one in order to get the other. That’s just not true. Only identity-based security has any effect on privacy, and there are limitations to that approach. Let me give you an example. Since 9/11, approximately two things have improved airplane security: reinforcing the cockpit door, convincing

See, Schneier, page 10

Data Breach Response Solutions from the organization you can trust.

For more than 100 years, Equifax has been the trusted repository for private consumer data, securely managing and protecting confidential information for more than 230 million individuals.

Public and private organizations, employers and consumers alike call on Equifax more than 5 million times each month to accurately verify personal identities.

These are a few reasons why Equifax is called on most often to support organizations, large and small, victimized by a data breach:

Most Experienced - Equifax’s team has supported more than 1,100 events over the last 4 years

Most Flexible

- ID Protection products and capabilities
- Breach Response Services
- Program option pricing
- Program and product fulfillment

Most Secure and Stable

- The only US based, publicly traded (NYSE: EFX), national credit reporting company, Equifax currently stores, manages, maintains, secures and protects the consumer data used in delivering ID Protection and ID Theft Detection/Prevention solutions.

For more information, e-mail us at: psol@equifax.com Or call us at: (866) 510-4211
passengers they need to fight back, and—maybe—sky marshals. Note that those three things have absolutely no effect on privacy. And many other forms of security have no effect on privacy: door locks, burglar alarms, tall fences. ID checks, databases, watch lists: those have a huge privacy impact, and they do almost nothing to improve security. The real opposites are liberty versus control.

**IAPP:** Is privacy the new environmentalism?

**Schneier:** Yes, and data is the pollution problem of the Information Age. Think about it. All computer-mediated processes produce data. Unless dealt with, it stays around. And its after-effects can be pretty toxic. And, just as 100 years ago we ignored pollution in our rush to build the industrial age, today we’re ignoring data in our rush to build the Information Age. And, I believe, 100 years from now our great-grandchildren will look back at the decisions we made and wonder how we could have been so ignorant and short-sighted.

**IAPP:** What gives you hope for the future of the information economy?

**Schneier:** I have a lot of faith in our species’ ability to get this right eventually. Yes, we’re getting it badly wrong now, and will continue to get it badly wrong in the short term. But as Martin Luther King Jr. said: “The arc of history is long, but bends towards justice.” Twenty years from now I believe we will have more liberty, more privacy, and more security than ever before.

**IAPP:** Can you give us a preview of your address for the IAPP Privacy Summit?

**Schneier:** I just did. I will be talking about the technological threats to privacy, the economic motivations that exacerbate these threats, and what’s likely to happen to privacy in the near future.
Thank you to the IAPP Privacy Summit 2009 sponsors

Microsoft
at&t
Baker & McKenzie
PricewaterhouseCoopers
3M
Booz | Allen | Hamilton
delivering results that endure
Ernst & Young
Quality In Everything We Do
Idexx
KPMG
LexisNexis
Symantec
TRUSTe
Venable, LLP

www.privacysummit.org
February • 2009

In the session The Privacy Act: Advanced, Ken Mortensen said changes to the 1974 Privacy Act are coming. He said his recent conversations with privacy-interested legislators tell him that they are interested in updating the three-decades-old act to include provisions on dealing with modern data and databases, among other considerations.

“I would bet good money we’ll see changes toward the end of the first term of the new Congress.”

Recently, our non-covert surveillance cameras captured the action at the Practical Privacy Series: Government in Washington, DC.

(Above) Leslie Harris, president and CEO of the Center for Democracy and Technology, delivered the keynote address.

(Above) Hundreds of Capitol-area privacy pros attended the Practical Privacy Series event in December.

(Above) In the session The Privacy Act: Advanced, Ken Mortensen said changes to the 1974 Privacy Act are coming. He said his recent conversations with privacy-interested legislators tell him that they are interested in updating the three-decades-old act to include provisions on dealing with modern data and databases, among other considerations.
The Artificial Divide between Privacy and Security

Anatomy of a Privacy Program

The Privacy Act: Advanced

Federal Web Sites: Best Practices for Compliance and Protecting Privacy in a Web 2.0 World

Beyond FAR: Implementing Privacy Safeguards in Vendor Relationships

Spice Up Your Privacy Program: Getting Employees Engaged

(Please see the illustrations for panelists’ approaches and their success stories.)

NEVER ARGUE WITH THE DATA
Nine out of 10 UK citizens feel data protection is as important as crime. That’s according to the Information Commissioner’s annual tracking survey of 1,000 people.

Source: Telegraph.co.uk

THREE’S COMPANY?
Only 45 percent of organizations include information security requirements in their contracts with third-parties, and nearly one-third do not review or assess how contractors are protecting their information.

Source: Ernst & Young 2008 Information Security Survey

EMPHASIS ON THE “I”
IAPP members represent 47 nations on six continents.

Source: IAPP

SHARING HAS SOCIETAL VALUE
Academic, legal and privacy communities are beginning to acknowledge a greater social benefit to data sharing, such as that seen on social-networking sites. Find out more at: www.1to1media.com/view.aspx?DocID=31350.

Source: Inside 1to1: Privacy

(Above) In the session Spice Up Your Privacy Program, panelists from the FTC, the FDIC, and the TSA shared their creative approaches toward getting employees engaged in privacy protection. Peter Pietra of the Transportation Security Administration told attendees how his Privacy Man poster series helped him communicate the importance of privacy to 55,000 employee in 460 locations across the country, 80 percent of whom have no or limited computer access. Pietra said the series garnered an “enormous response.”

(Above) Nat Wood of the Federal Trade Commission and Steven Lott of the FDIC shared their successes implementing “Privacy Week” in their organizations. Wood used this “Handle with Care” image as one of a battery of materials to raise awareness.
FRANCE

By Pascale Gelly

Online games, Internet service providers, and the Council of Europe

The Council of Europe, which hosted the last international conference of privacy commissioners in Strasbourg, has issued two sets of guidelines for the online game industry and Internet service providers “to encourage, respect, and promote privacy, security, and freedom of expression when, for example, accessing the Internet, using e-mail, participating in chats or blogs, or playing Internet games...”

www.coe.int

Freedom of speech v. privacy

The head of a precinct did not manage to convince a publisher to remove statements he found disparaging made about him on a blog. To get the article removed entirely from the site, he sued the hosting company in an emergency proceeding, claiming his right to object to data processing on legitimate grounds under the Data Protection Act.

He failed to succeed, as the Paris court considered that such a request would undermine the rules protecting freedom of speech. The offended individual should have sued the blog publisher, not the host.

Professional correspondence, or not? Questions remain.

A civil servant subject to disciplinary proceedings found in his personnel file a copy of an e-mail he had sent to a friend and colleague in the IT department of the same organization. He filed a criminal claim for violation of the duty of secrecy of private correspondence. The message content was half professional-half personal, but the message title did not indicate any personal content.

The court of first instance ruled that in order to determine whether an e-mail is personal, one must look not only at the purpose of the e-mail, but also at the intention of the interested parties. In this matter, the IT employee had sent to several people an e-mail under the title “budget.” The civil servant did not use the “reply to all” function, rather, replied only to the sender, splitting his answer in two parts: one personal and one professional. The management obtained the e-mail by applying pressure on the IT employee, who was reluctant to provide it. All these ele-
ments showed that this e-mail was intended to be a private e-mail, which should not have been accessed by the management. The court held that the secrecy of correspondence had been violated.

Opt-in for Bluetooth advertising on cell phones

After a large supermarket chain launched a large marketing campaign in several French towns, the CNIL issued an opinion about the emerging marketing practice of sending ads to cell phone holders using geo-tracking technology that detects phones’ locations using activated Bluetooth functionality. Cell phones’ “MAC” address and Bluetooth identifiers are deemed to be personal data. As a consequence, phone holders must provide prior consent before direct marketing materials may be sent to their cell phones.

The CNIL assessed methods for collecting individuals’ consent. Sending messages to all phone holders entering into a Bluetooth coverage zone in order to request consent was deemed inappropriate. The CNIL favors a solution whereby only individuals interested in the advertising would receive the messages. Users could express such interest by bringing their phones close to an advertising panel in order to receive the ad.

Pascale Gelly is a partner at Cabinet Gelly. She can be reached at pg@pascalegelly.com.

INTERNATIONAL

By John W. Kropf, CIPP/G

Global privacy: Strasbourg calls for European-based international privacy standards

The data protection authorities (DPAs) of France and Germany co-hosted the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, France, late last year. During the first two days, more than 600 privacy professionals from government, DPAs, academia, and the private sector participated in open sessions. Meetings of the commissioner’s subgroups—the Asia Pacific Privacy Association (APPA) and the International Working Group on Data Protection in Telecommunications (the “Berlin Group”)—preceded the event.

See, Global Privacy Dispatches, page 16

“Macau was invited to re-apply on the condition of certain developments in its privacy framework.”
A closed session devoted to administrative measures and the commissioners’ discussion of conference resolutions comprised the last half day. Invited by the German and French co-hosts, officials from the U.S. Department of Homeland Security (DHS) and the U.S. Federal Trade Commission (FTC) followed the proceedings as “official observers.”

The Commissioners’ members began the closed session by considering applicants for new membership. They granted full member status to: Croatia, Burkina Faso, and the German state of North Rhine Westphalia. Macau was invited to re-apply on the condition of certain developments in its privacy framework.

Spain was added on the credentials committee for the coming year.

By the end of the meeting, the group had adopted six resolutions. Of greatest significance was a resolution calling on the United Nations (UN)—through the International Law Commission (ILC)—to set forth a UN convention on a binding set of international privacy standards. The resolution, co-sponsored by Spain and Switzerland, is more explicitly Euro-centric than similar resolutions passed during the last three years, stating that such a convention should be based on the European Convention 108.

The commissioners adopted two resolutions supporting outreach efforts. The first called for the creation of a permanent Web site to support the group and its future conference. A representative from the Organisation for Economic Co-operation and Development (OECD) demonstrated what the Web site might look like. The site would likely contain information on future conferences and would serve to archive commissioners’ past resolutions.

The Australian privacy commissioner also proposed a resolution, ultimately adopted, calling for the exploration of a day or week to commemorate a recognition of privacy. Currently, the EU recognizes 28 January as its International Privacy Day, while the Asia-Pacific Privacy Association (APPA) organizes Privacy Awareness Week (PAW) each year during the last week in August. A working group will be established to reconcile the different dates.

The group also adopted a resolution proposed by the privacy commissioner of New Zealand for the creation of a steering group to coordinate commissioners with international forums—including
OECD, ISO, the Council of Europe, APEC, the UN International Law Commission, and, by amendment, UNESCO.

The last two resolutions expressed concerns over privacy protections for social networking and children’s activities on the Internet.

While the resolutions have no legally binding effect, they are nonetheless an expression of those commissioners who meet the group’s membership criteria. The resolutions can be viewed at the Conference’s official Web site: www.privacyconference2008.org.

This year’s conference will be held in November in Madrid.

John Kropf is the deputy chief privacy officer and senior adviser for international privacy policy at the U.S. Department of Homeland Security’s Privacy Office. The views expressed here are his and not those of the Department of Homeland Security or the U.S. Government. He may be reached at john.kropf@dhs.gov

MEXICO

By José-Luis Piñar Mañas

Federal Constitution reformed to recognize the right to data protection

Mexico passed an important constitutional reform on 12 December 2008, whereby the text of the Federal Constitution incorporates the express recognition of the fundamental right to the protection of personal data. For such purpose, a second paragraph was added to article 16, which establishes the following:

All persons are entitled to the protection of their personal data, to the access, rectification and cancellation thereof, and to manifest their opposition, under the terms provided by law, which shall establish the cases exempted from the principles governing the processing of data, due to reasons of homeland security, public order, security and public health provisions, or for the protection of third-party rights.

Thus far, the right to data protection had been incorporated partially in several laws. Prominent among them is the Federal Act on Transparency and Access to Government Public Information 2002, including a specific chapter regulating data protection. The Federal Institute of Access to Information (IFAI) is the agency entrusted with ensuring the right to data protection in relation to government entities. Also, nearly all of the states have passed laws on Transparency and Access to Information regulating this matter.

A reform of article 73 of the

See, Global Privacy Dispatches, page 18
Constitution was also passed in order to give the Union Congress express powers so that it may prepare and pass a federal law for the protection of personal data in the possession of individuals and private entities. With the constitutional reforms that were just passed, Mexico is now at the forefront of the countries with constitutional recognition of the right to data protection.

**SPAIN**

*By José-Luis Piñar Mañas*

**Privacy Protection in social network services**

An important Resolution on Privacy Protection in Social Network Services was adopted at the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg on 17 October 2008.

The resolution follows the guidelines set in the “Report and Guidance on Privacy in Social Network Services” (Rome Memorandum) of the 43rd meeting of the International Working Group on Data Protection in Telecommunications (3-4 March 2008), and in the ENISA Position Paper No. 1 “Security Issues and Recommendations for Online Social Networks” (October 2007). It includes a number of recommendations that must necessarily adopt the form of legal regulations or must be incorporated into the privacy policies of service providers. They represent a significant stride forward because, at a worldwide level, steps have been taken with the firm goal of minimising the risks that social networks pose for data protection. And these risks are not always easy to imagine.

The starting point is the fact that “individuals face the possible loss of control over how data will be used by others once they are published on the network: while the ‘community’ basis of social networks suggests that publishing one’s own personal data would just resemble sharing information with friends as if used face-to-face, profile information may in fact be available to an entire subscriber community (numbering in the millions).”

The resolution includes two recommendations for users and 10 for service providers. The former have to do with the publication of information, and they point out that “users of social network services should consider carefully which personal data—if any—they publish in a social network profile. In particular, minors should avoid revealing their home address or telephone number. Besides, users should also respect the privacy of others. They should be especially careful with publishing personal information about somebody else (including pictures or even tagged pictures) without that other person’s consent.

In relation to service providers, it is assumed that providers of social network services have a special responsibility to consider and act in the interests of individuals using social networks. In addition to meeting the requirements of data pro-

See, *Global Privacy Dispatches*, page 20
LuciData, Inc. provides companies with the complete lifecycle of Data Security and privacy. Whether it is Computer Forensics related to an incident, proactively identifying internal risks, or providing forensic training to your in-house security team, we can help.

We recognize that resolving the entire problem is more important than just treating the individual symptoms of an incident.

LuciData, Inc. is a recognized industry leader with extensive experience and a reputation for handling the most complex challenges with skill and efficiency.

To learn more contact us:
www.lucidatainc.com
1-866-LUCIDATA

---

KROLL

DATA BREACH & IDENTITY THEFT SOLUTIONS

- Prepare
- Contain
- Respond
- Restore
- Retain

Visit us at Booth #214 during the Privacy Summit in Washington, D.C.
tection law they should also implement the recommendations that are included in the resolution. Said recommendations refer to the following aspects:

1. **Privacy regulations and standards.** Providers operating in different countries or even globally should respect the privacy standards of the countries where they operate their services.

2. **User information.** Providers should inform their users about the processing of their personal data in a transparent and open manner.

3. **User control.** Providers should further improve user control over the use of their profile data by community members. As a minimum, opt-out for general profile data, and opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data should be offered.

4. **Privacy-friendly default settings.** Providers should offer privacy-friendly default settings for user profile information. Such settings must be specifically restrictive when a social network service is directed at minors.

5. **Security.** Providers should continue to improve and maintain security of their information systems and protect users against fraudulent access to their profile.

6. **Access rights.** Providers should grant individuals the right to access and, if necessary, correct all their personal data held by the provider.

7. **Deletion of user profiles.** Providers should allow users to easily terminate their membership, delete their profile and any content or information that they have published on the social network.

8. **Pseudonymous use of the service.** Providers should enable the creation and use of pseudonymous profiles as an option, and encourage the use of that option.

9. **Third-party access.** Providers should take effective measures to prevent spidering and/or bulk downloads (or bulk harvesting) of profile data by third parties.

10. **Indexibility of user profiles.** Providers should ensure that user data can only be crawled by external search engines if a user has given explicit, prior, and informed consent. Non-indexibility of profiles by search engines should be a default setting.

José-Luis Piñar Mañas, Ph.D. is an attorney at Piñar Mañas & Asociados Law Firm, and a professor of administrative law. He also is the former director of the Spanish Agency for Data Protection and former Vice-Chairman of the Article 29 Working Party and Honorific President of the Ibero-American Network of Data Protection. He can be reached at jlpinar@pmasociados.com.
What are you reading?

The Privacy Advisor asked Harriet Pearson what she is reading these days. In preparation for the Privacy Book Club session at Summit next month, Harriet just finished Understanding Privacy by Dan Solove. Here’s what she said about it:

“A book like Solove’s comes along once in a generation. It starts with a usefully succinct yet comprehensive review of the major theories of privacy—e.g. the right to be left alone; right to control information about oneself; right to prevent interference with one’s person. But the heart of the book, and its unique contribution, is how Solove organizes the complex concept of privacy into a practical theoretical framework that a privacy pro, policymaker, lawyer or judge can use to analyze and act on the specific issues that confront them. He does all this in 200 pages that I’ve already highlighted and referred to multiple times. Understanding Privacy has earned a place in the bookcase closest to my desk.”


Go here to download a segment of the book: http://docs.law.gwu.edu/facweb/dsolove/Understanding-Privacy/.
With a new Administration, a significantly different Congress and a wide range of new rules and upcoming legislation, privacy and security professionals will continue to have their hands full in 2009 with new developments. Here are a few of the main items we’ll be watching.

1. Increasing government enforcement

Despite the substantial array of privacy and security laws and regulations, at all levels of government, enforcement of privacy and security laws has remained nominal. Some agencies, like the Federal Trade Commission, have brought a modest number of high profile enforcement actions. Other agencies, like the HHS Office of Civil Rights (for the HIPAA Privacy Rule) and the various federal agencies responsible for Gramm-Leach-Bliley Act enforcement, have done virtually nothing on enforcement.

There are significant reasons to anticipate new enforcement policies in the year ahead. First, even in 2008,
there started to be some movement towards additional enforcement. In the health care industry, for example, we saw the first HIPAA penalty, brought against Providence Health Systems. [See Nahra, “The HIPAA Enforcement Era Begins,” Privacy In Focus (August 2008), available at www.wileyrein.com/publication_newsletters.cfm?sp= newsletter&year=2008&ID= 10&publication_id=13717& keyword=providence.]

There also are continued calls for additional enforcement, from Congress and a wide range of privacy advocates. In the Obama Administration, enforcement of privacy laws is likely to be a significant priority. Additional enforcement resources for the Federal Trade Commission were a component of the Obama campaign platform. There is a virtual guarantee that the new Administration will take a more aggressive approach on enforcement of the HIPAA rules. Accordingly, we can expect a general increase in enforcement activity in 2009, although this is likely to be a stream rather than a flood.

Key Action Item - Because of the new likelihood of enforcement action, companies should pay particularly close attention to complaints about privacy and security, and should act aggressively to mitigate any security breaches or other potential harms from privacy and security failures. Also, pay close attention to marketing issues—this is a key area of ongoing controversy, and one where privacy advocates are particularly aggressive in pushing for more enforcement.

2. The FTC’s challenging “red flags”

In terms of new regulatory obligations, the FTC’s “red flags” rule stands far and away as the most broadly applicable and challenging regulation on the horizon. The red flags rule, one of the last FTC rules to be promulgated under the Fair and Accurate Credit Transactions Act (FACTA), imposes obligations on “financial institutions and creditors” to develop an “identity theft red flags program.” While the “financial institution” definition is somewhat technical and therefore very limiting, the concept of

“In terms of new regulatory obligations, the FTC’s “red flags” rule stands far and away as the most broadly applicable and challenging regulation on the horizon.”

See, What’s ahead in 2009, page 24
“creditors” has potentially broad application; moreover, the FTC has taken a surprisingly broad view of its own rule, such that virtually any company in any industry that provides services in advance of payment may face obligations under this rule.

The FTC, despite its scary pronouncements on the scope of the rule, also has acknowledged that its interpretation will impact numerous companies not accustomed to such regulation. Accordingly, the FTC has moved a November 1, 2008 effective date back to May 1, 2009, to give companies an additional opportunity to meet their compliance obligations on the “identity theft program” aspects of this rule (other components still have a November 1, 2008 compliance date). While the extension is appreciated, many companies will face challenges in meeting this deadline.

Key Action Item - Companies in virtually all industries face the possibility of being identified as creditors. The first step for any company—which needs to be taken immediately—is to determine the situations in which the company issues any kind of credit, interpreted as broadly as providing services in advance of payment. In the FTC’s view, these companies are “potentially” covered by the rules. The second step in the analysis is the hard one—does a company have “covered accounts,” meaning specific kinds of transaction accounts, or other accounts where there is a credible threat of identity theft. The main task for most companies will be to conduct a risk assessment of their accounts, to determine whether there are credit arrangements that require companies to adopt a full scale red flags program.

3. Identity theft as an enforcement priority

The broad scope of the red flags rule reflects an ongoing and growing concern about the problem of identity theft. The enforcement effort directed at fighting identity theft continues to expand. For example, the Department of Justice and the Federal Trade Commission recently released an updated status report on overall efforts directed against identity theft. [See “Combating Identity Theft: A Strategic Plan,” available at www.ftc.gov/os/2008/10/081021taskforcereport.pdf.] In the press release accompanying the status report, the FTC and the Department of Justice made clear that “Government
and the private sector, working together with consumers, must remain vigilant and adaptable as new generations of identity thieves and techniques develop over the coming years.”

In addition, we also are seeing an increased focus on a newer form of identity theft—medical identity theft. The U.S. Department of Health and Human Services’ Office of the National Coordinator for Health Information Technology and the FTC recently held a “Town Hall” meeting on medical identity theft. The general conclusion of the meeting is that there is ongoing confusion about medical identity theft, and few effective means of fighting identity theft. (A “report and roadmap” from this Town Hall meeting is expected to be published this winter.) In addition, the movement towards electronic medical records creates the possibility that the problem with medical identity theft will get worse (although there clearly are some who think that electronic medical records can help solve this problem in the health care industry). As a general matter, industry concerns with identity theft, whether medical or otherwise, must remain high, as identity theft is the main potential and concrete “harm” that can be suffered as a result of security breaches.

Companies need to continue an aggressive fight against identity theft and should broaden their scope of review to include not only credit-related risks but other forms of identity theft as well.

Key Action Item - One of the primary conclusions from recent identity theft cases indicates that many identity theft schemes result from improper activity by insiders. Accordingly, companies need to focus extra attention on how data access is controlled within companies. Identity theft concerns also reflect a broader set of privacy-related problems caused by corporate insiders, such as the well-publicized events affecting the UCLA Medical Center, where dozens of employees reviewed celebrity medical records for improper or inappropriate purposes. So, companies need to focus on reviewing employee access controls on the front end, increasing sanctions and training related to improper actions, and, most importantly, must review how best to conduct ongoing auditing and monitoring of employee access, particularly in industries where customer service representatives and others have access.

See, What’s ahead in 2009, page 26
What’s ahead in 2009
continued from page 25
to large amounts of customer or employee data.

4. Litigation developments expected

We also can expect continued efforts by plaintiffs’ attorneys to poke holes in the existing cases that preclude liability absent a showing of actual harm. In a wide range of cases across the country, the threat of potential loss has not been found sufficient to permit a case to go forward. A lack of actual damages—even in the face of clear security breaches—is now the primary hurdle in most privacy and security cases.

Despite this strong line of precedent, the continuing spread of security breaches, particularly on a large scale, is making multiple class action filings almost commonplace when breaches are publicly disclosed. Moreover, many of the new laws (including some pending proposals) incorporate a private cause of actions and/or statutory damages as a means of increasing the use of these private enforcement tools.

What can we expect on the litigation front? First, we likely will see an increased use of “negligence” theories to bring cases, relying on existing regulatory or industry standards. We have seen in recent years a series of cases where a common law negligence approach has been used to start a case—by developing the framework for a cause of action.

Beyond the negligence theory, the key issue is still damages. While the negligence theory allows a complaint to get filed, there hasn’t been any clear evidence (yet) that this theory is enough to overcome the damages hurdle. Moreover, the few published cases to date typically have involved “single injury” situations, where one (or a small number) of individuals have been the potential victims of a privacy or security breach.

Accordingly, many uphill challenges remain to bringing successful privacy/security suits (or, conversely, lots of defenses still exist, even when companies have not behaved well). But, as breach cases continue to grow, plaintiffs are continuing to push the envelope on creative theories concerning how these compliance failures translate to consumer injuries.

Key Action Item - Watch for the breakout case, which could open the litigation

See, What’s ahead in 2009, page 28
How would your organization score on the Privacy Maturity Model?

Avior Computing & Minnesota Privacy Consultants team to create the industry’s first Web-Based solution for Worldwide Privacy Assessments and Industry Benchmarking.

Are you challenged by the myriad of global privacy regulations that your organization must comply?

Benefits:
- All major privacy laws integrated into a single assessment platform
- Board reports of rank-ordered enterprise privacy risks
- Simple automated scheduling and reporting
- Easy to implement and use

Privacy Laws of...
- Europe
- US
- HIPAA
- GLBA
- SSN laws
- Canada
- Australia
- Argentina
- State breach notification laws
- ...CA1386
- and many others...

COBIT
GAPP

Please contact us for more information at bbeck@aviorcomputing.com or cline@minnesotaprivacy.com

MEDIAPRO®

Employee Privacy & Security Training

Privacy Directions™
- Employee Awareness
- Human Resources
- Information Technology
- Call Centers
- Sales & Marketing
- Hospitality
- COPPA

Security Directions™
- Employee Awareness
- Security Awareness with Privacy Principles
- Awareness and Reinforcement Materials and Templates
- Employee Blogging
- PCI Awareness

Smart. Safe. Secure.
Award-Winning e-Learning & Awareness Solutions

For a FREE DEMO
Call (800) 955-3014
www.MediaPro.com
floodgates. The critical cases to watch will be those that combine a negligence approach with a credible damages argument, on a class-wide scale. And pay special attention to any laws that include statutory damages—eliminating the need to prove actual damages. While Congress “fixed” the problem with statutory damages in the FACTA credit card “expiration date” disclosure suits, we can’t expect this kind of action in the future. The increasing likelihood of privacy and security claims that can survive initial motions in court also means that it is critically important for companies to document their ongoing compliance efforts, so that they can demonstrate their actions to meet the variety of relevant requirements.

5. Expanding data security obligations

The last critical issue for 2009 will involve ongoing developments related to the protection of customer and employee information—the “security” side of the privacy and security field. Clearly, there is a substantial cross-over between privacy and security. Some areas—like the various marketing rules—fall obviously onto the privacy side. Other issues—mainly related to breaches—could be considered either privacy or security issues. But, it is clear that the regulatory obligations related to security are growing and that, for many companies, these security obligations will be both more burdensome and more broadly applicable. Accordingly, analyzing and updating information security programs needs to be a key consideration for any company.

For many years, a reasonable and appropriate information security program has been a requirement for any company that maintains personal information—essentially, every company. [See Nahra, “Effective Security Practices Now a National Requirement,” Privacy In Focus (June 2009), available at www.wileyrein.com/Effective_Security_Practices.] Beyond this “general” obligation, we have seen the implementation of specific security requirements on an industry-specific basis (such as the HIPAA Security Rule and the Gramm-Leach-Bliley safeguards rule). Next, we saw the development of a nationwide matrix of “security breach notification laws”—requiring consumer notification in the event of certain security breaches. While these laws did not, by themselves, impose specific security mandates, they did create obligations—for all businesses—in the event of a security failure.

“This law could require many companies to alter their behavior, particularly in connection with e-mail transmissions.”
Now, there are two key developments that are imposing specific security details on most companies. First, the “Payment Card Industry” (PCI) security standards apply broadly to any company that takes credit cards as a means of payment. The PCI security principles are not new, but are becoming increasingly detailed and are being followed and monitored on an increasingly aggressive basis. A wide variety of materials about the PCI standards (including the recently released October 1, 2008 guidelines) is available at www.pcisecuritystandards.org/.

Most recently, we are seeing various new state laws that impose specific and detailed security obligations. For example, a new Nevada obligation, effective October 1, 2008, requires that “A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.” This law could require many companies to alter their behavior, particularly in connection with e-mail transmissions.

A new Massachusetts law imposes even broader obligations. In fact, Massachusetts has now imposed the most substantial set of security practice obligations applicable to businesses in all sectors. This law was scheduled to take effect on January 1, 2009, but this deadline recently was extended until May 1, 2009. Because the Massachusetts law has broad applicability, virtually any company that does business with a Massachusetts resident needs to be concerned about these requirements. While some of the requirements are straightforward (and consistent with the FTC’s earlier views on a reasonable and appropriate program), other requirements (such as specific encryption obligations and physical access restrictions) likely will require many companies to develop new security solutions.

Key Action Items - These new obligations require an overall review of a company’s information security practices. At a minimum, if you haven’t re-assessed your security program in the last two years, you need to do so now. Also, unless your business is restricted to a single state or a small region, make sure you understand the full set of obligations that you face under these laws. Then, focus attention on the primary areas of risk—make sure your employees are trained well, and that your information is protected as best as well reasonably can. Remember—the biggest risk is not violating these rules in the abstract—it’s the additional risk in the event of a breach if you haven’t met a required standard.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, DC, where he specializes in privacy and information security litigation and counseling. He is chair of the firm’s Privacy Practice. Kirk is an Ex Officio member of the IAPP Board of Directors, and is the editor of the Privacy Advisor newsletter.
Who’s monitoring your Web Governance policy?

Protect your website with automated Privacy Compliance monitoring from HiSoftware.

Sure you have a Web Governance strategy, but who’s keeping an eye on the thousands of pages on your internet and extranet sites? HiSoftware’s automated Web compliance solutions for Privacy and Accessibility monitoring can help. With HiSoftware receive reports on the status of your site pages against standard regulatory and custom compliance policies when you need them - alerting you to potential issues before they become a problem.

Visit HiSoftware during the IAPP Privacy Summit in Washington, DC at Booth 209 and inquire about setting-up a Free Sample Scan of your site.

www.hisoftware.com
info@hisoftware.com
Americas 1 888 272 2484, +1 603 578 1870
Europe, MiddleEast & Africa +33 (0) 6 72 51 95 21

IdentityFinder Data Loss Prevention

Find and protect Personally Identifiable Information before it’s too late

Discover:
Social Security Numbers
Passwords
Credit Cards
Bank Accounts
Dates of Birth
Medical Records
Financial Data
and more...

Shred | Encrypt | Redact | Quarantine

www.identityfinder.com
Early in his career, Christopher Kuner cut his teeth on European data protection law while working at a large German firm. He worked in corporate law, but kept seeing data protection questions pop up as companies merged and pooled databases. “Gradually,” he says, “the data protection issues began eating up all my time.”

Some years have passed, privacy has entered the mainstream, and the same issues continue to eat Kuner’s time. It’s his full-standing specialty at Hunton & Williams, where he heads the International Privacy and Information Management Practice from his office in Brussels.

Recently Kuner released the second edition of his book European Data Protection Law: Corporate Regulation and Compliance. The 550-page tome covers European data protection law with a focus on areas of interest to companies. Since the first edition in 2002, “privacy has obviously exploded,” says Kuner. Because of that, the new edition is double the size with a greatly expanded scope. European data protection supervisor Peter Hustinx wrote the foreword. Recently, the book became the first in-depth treatise on European data protection law to be published in Chinese.

For more information: www.oup.com/uk/catalogue/?ci=9780199283859

“Kuner’s diligence is evident in his research, his skill demonstrated by the book’s accessible prose, and his practitioner’s sensibilities shown by his practical explanations and reference to the underlying texts. This book is a must for any serious privacy practitioner’s library.”

—D. Reed Freeman, Partner, Kelley, Drye & Warren LLP

Learn the latest on privacy without ever leaving your office.

Visit the IAPP’s online Educational Library.

Did you miss an audio conference? Need to study for your privacy certification exam? Didn’t catch a particular session at a recent IAPP event?

Our most popular conference sessions, audio conferences and certification training materials are available for purchase.

The IAPP Educational Library is your one-stop resource:

- Earn CPE credits
- Create your own privacy library
- Study for privacy certification
- See what you missed at IAPP conferences
- Catch up on the latest audio conference

Earn CPE credits while you learn!

Each product you buy is eligible for credits toward your continuing privacy education (CPE) requirements.

www.privacyassociation.org/edulibrary
Privacy News

Kuner reviewing EU directive

Chris Kuner, head of Hunton & Williams’ International Privacy and Information Management Practice, has been appointed to a five-person committee tasked with reviewing the EU Directive. The group will assist the European Commission in the preparation of legislation or in policy definition.

The volunteer members of the group, known as GEX PD, were chosen based on their personal competence, professional experience and commitment to data protection matters. Kuner was named the “go-to person for EU privacy” in Computerworld’s survey of the best privacy advisers of 2008 and 2007, and was named a leader in his field in Chambers Global in 2006, 2007, and 2008.

The GEX PD first met on 4 December, at which time they identified five main categories of topics to be addressed in the coming months:

1) Implementation of the Data Protection legal framework (e.g. notifications, enforcement, mutual recognition, lead regulator);
2) Data processing in a globalised world (e.g. applicable law, international transfers)
3) Legal issues (e.g. definitions, scope)
4) Government access to data and its limitations
5) Consumers’ awareness and individuals’ rights

Members will produce a short discussion paper on some of the specific topics within the first main category. The group will discuss the papers during the next GEX PD meeting on 19 February.

Privacy Litigation Task Force

San Diego-based Foley & Lardner, recently ranked among the top 10 Best Privacy Advisers in 2008 by Computerworld, has established a Privacy Litigation Task Force to help its clients address the growing threat of privacy-related litigation. “Being able to provide these unique services is extremely important as more companies are faced with privacy and information security incidents,” said Andrew Serwin, co-chair of the task force. Other team members include Eileen Ridley, Michael Tuteur.

The team will assist clients in addressing litigation arising from security breaches; improper exporting and disclosure of information; improper delivery of commercial e-mails; violation of state medical privacy laws, and other matters related to the disclosure of e-mails and personally identifiable health and financial information.
What’s in a name?

A growing number of organizations recognize the link between information security and reputation. That’s according to Ernst & Young’s 2008 Global Information Security Survey, which polled 1,400 senior executives in 50 countries.

Eighty-five percent of respondents indicated that a security incident would have a significant impact on reputation and brand, while 72 percent felt such an incident would most impact revenues.

“A good brand and reputation can take years to build but can be severely damaged or even destroyed by a single security incident,” said Paul van Kessel of Ernst & Young’s Technology and Security Risk Services. “The media coverage surrounding security breaches underscores just how devastating these failures can be to a firm’s reputation.”

The study also revealed that, despite the economic downturn, 50 percent of respondents plan to increase their security budgets.


Breach insurance

“We’re very pleased to bring DataBreach into the marketplace.”

Specialty insurance products provider Markel has released an information risk and privacy liability insurance product, DataBreach.

“We’re very pleased to bring DataBreach into the marketplace,” Markel Chief Underwriting Officer Gerry Albanese told Insurance Business Review. “With identity theft on the rise, the timing couldn’t be better.”

The product provides coverage for liabilities arising out of the breach of a company’s duty to protect confidential information and extends to a business liability arising out of an employee’s misuse of his/her access to confidential information.
Let’s go surfin’ now

Level 9 Technology has launched ArmorSurf, a free web browser that lets users surf in private. When ArmorSurf’s IP Masking feature is enabled, users’ surfing activities become anonymous and untraceable. In addition, ArmorSurf automatically encrypts and secures browsing history, cookies, cache, auto-complete history, favorites, and other personal information. The browser has an encrypted file manager that stores all imported and download files.


Kill switch

Ericsson has introduced an anti-theft module for commercial laptops. The Mobile Broadband Module lets users send a text message to render the laptop useless in the event it has been lost or stolen. The module also includes a global position system. Ericsson plans to introduce similar modules for business laptops in late 2009.

In the Privacy Tracker this month...

One of the technology sector buzzwords for 2008 was “cloud computing,” or “the Cloud.” The Cloud really means access to data processing and storage via the Internet. Companies such as Google, Apple, Dell, Amazon, Hewlett Packard, Oracle and Microsoft are betting that individuals and businesses will want to store all of their e-mail, contact lists, family photos, documents and other vital information in the Cloud. The seductiveness of the Cloud is that it represents, and is being marketed as, a computing utopia, a world where computers never crash, and where all vital information is easily accessible via any Internet connection, is made indestructible through redundancy and is very secure locked inside a specialized company’s heavily fortified physical data center.

In this month’s Privacy Tracker article, Bart W. Huffman and Erin Fonte of Cox Smith, discuss the rise of cloud computing, explain the current move toward adoption of cloud computing in the business context, and highlight unique business and legal issues that must be considered when a business entity decides to move some or all of its data “into the Cloud.”
Pappachen appointed chief privacy officer

George Pappachen has been named chief privacy officer of the Kantar Group. In the newly-created position, Pappachen will implement a Group-wide privacy and data protection policy and will also work with clients on these issues. Pappachen joins Kantar after two years as director of privacy and public policy at Kantar’s research arm, Safecount.

“It is an opportunity to introduce best-in-class practice to one of the world’s biggest data-based operations.”

“Privacy and data protection issues are top of mind for many consumers and will become so for many more,” said Kantar Group Chief Executive Eric Salama. “I am excited to develop the work I have done with Safecount onto the broader Kantar Group platform, especially at a time when privacy is becoming business-critical for ourselves and our clients,” said Pappachen. “It is an opportunity to introduce best-in-class practice to one of the world’s biggest data-based operations.”

New ICO named

Pending House of Commons approval, Christopher Graham will become the UK’s next information commissioner. Graham will replace Richard Thomas when he retires in June. Currently, Graham is director general of the Advertising Standards Authority, a position he has held for nine years. “The information commissioner is so much at the centre of debates on information security, privacy, better government and the right to know,” Graham told the Guardian, “I am keen to take on this new challenge.”

The most important conference of 2009 for Canada’s privacy profession.

IAPP CANADIAN PRIVACY SUMMIT 2009

29 April – 1 May
InterContinental Toronto Centre

Three days of EDUCATION, NETWORKING and DISCUSSION of the issues that matter to you.

REGISTER NOW www.privacyassociation.org
## Calendar of Events

### FEBRUARY

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Certification Testing – Seattle, WA</td>
<td>Certification Foundation - CIPP, CIPP/G and CIPP/C and CIPP/IT examinations</td>
</tr>
<tr>
<td>11</td>
<td>KnowledgeNet - Boston, MA</td>
<td>Topic: Privacy 2009: What’s Keeping You Up at Night?</td>
</tr>
<tr>
<td>11</td>
<td>KnowledgeNet - Dublin, Ireland</td>
<td>Topic: Benchmarking Privacy Around the World &amp; Data Loss Prevention</td>
</tr>
<tr>
<td>12</td>
<td>KnowledgeNet - Columbus, OH</td>
<td>Topic: Risk at home: Privacy and Security Risks in Telecommuting</td>
</tr>
<tr>
<td>13</td>
<td>KnowledgeNet - Cincinnati, OH</td>
<td>Topic: Risk at home: Privacy and Security Risks in Telecommuting</td>
</tr>
</tbody>
</table>

### MARCH

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-13</td>
<td>IAPP Privacy Summit</td>
<td>Washington D.C.</td>
</tr>
</tbody>
</table>

### APRIL–MAY

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
</table>
| 26-29| HCCA’s 13th Annual Compliance Institute | Caesars Palace, Las Vegas  
www.compliance-institute.org |

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
</table>
| 29-May 1 | IAPP Canadian Privacy Summit | Toronto, ON  
Details at www.privacyassociation.org |

### JUNE

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-18</td>
<td>Practical Privacy Series: Data Breach, Data Governance, Human Resources, Information Security</td>
<td>Silicon Valley, CA</td>
</tr>
</tbody>
</table>

### SEPTEMBER

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Privacy Dinner</td>
<td>Boston, MA</td>
</tr>
<tr>
<td>16-18</td>
<td>Privacy Academy 2009</td>
<td>Boston, MA</td>
</tr>
</tbody>
</table>

### DECEMBER

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Practical Privacy Series: Government</td>
<td>Washington, DC</td>
</tr>
</tbody>
</table>

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

## DON’T WAIT UNTIL YOUR COMPANY MAKES THE HEADLINES.

- A high-profile privacy breach can damage your company’s reputation.
- Experts estimate 70 – 80% of data security breaches are due to internal access to sensitive information.
- Sensitive data exists in many systems so access is difficult to control. Know where this information exists and who has access to it.

**Approva proactively notifies security professionals and business users of violations of privacy best practices within the application as well as the database.**

Learn how internal controls address the need for privacy controls.  
[www.approva.net/solutions/privacyprotectionandmonitoring](http://www.approva.net/solutions/privacyprotectionandmonitoring)
TRUSTe’s EU Safe Harbor Seal Certification

Accountability for cross-border data transfers

- Get ready for self-certification with the U.S. Department of Commerce
- Verify compliance with the Safe Harbor Framework
- Satisfy dispute resolution requirements for consumer complaints

Visit www.truste.com or contact Michelle Hines at 415.520.3402 or mhines@truste.com to get certified today.

PRIVACY PERSPECTIVES

News from the Office of the Privacy Commissioner of Canada

Want the inside scoop on what the Office of the Privacy Commissioner of Canada (OPC) is doing to protect and promote privacy rights in Canada and abroad?

Check out Privacy Perspectives, the new OPC e-newsletter!

Every issue contains:
- News about the OPC and the work it is doing
- OPC points of view on emerging privacy issues
- OPC employee perspectives

Plus, links and information highlighting:
- Hot privacy topics
- The latest OPC case summaries
- New tools and information

Read the current issue or subscribe at: www.privcom.gc.ca
Privacy Certification Exams 2009

Got goals? Get Certified.

Thinking about getting your privacy certification this year? Exams will be held in the following cities. Visit www.privacyassociation.org for specific dates and locations.

<table>
<thead>
<tr>
<th>JANUARY 2009</th>
<th>FEBRUARY 2009</th>
<th>MAY 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boston, MA</td>
<td>Seattle, WA</td>
<td>Chicago, IL</td>
</tr>
<tr>
<td>Dallas, TX</td>
<td>Victoria, BC</td>
<td>Denver, CO</td>
</tr>
<tr>
<td>Minneapolis, MN</td>
<td>New York, NY</td>
<td>Ottawa, ON</td>
</tr>
<tr>
<td>New York, NY</td>
<td></td>
<td>Toronto, ON</td>
</tr>
<tr>
<td>Ottawa, ON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Philadelphia, PA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Francisco, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toronto, ON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Washington, DC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MARCH 2009</th>
<th>JUNE 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago, IL</td>
<td>New York, NY</td>
</tr>
<tr>
<td>Los Angeles, CA</td>
<td>San Francisco Bay Area, CA</td>
</tr>
<tr>
<td>Washington, DC</td>
<td></td>
</tr>
</tbody>
</table>

Turn Marketing Compliance into a Competitive Advantage.

Are your marketing programs compromised by the iron fist of consumer contact compliance regulations? Gryphon Networks’ award-winning solutions help the world’s largest organizations loosen the grip, giving them a measurable competitive advantage. Visit us at the IAPP Privacy Summit, Booth #302, and we will show you how.

Register to win a free Risk Assessment.


Contact Gryphon Networks today: gryphonnetworks.com

<table>
<thead>
<tr>
<th>TELEPHONE</th>
<th>EMAIL</th>
<th>MAIL</th>
<th>SMS</th>
<th>FAX</th>
</tr>
</thead>
</table>

www.privacyassociation.org
AUGUST 2009
Seattle, WA

SEPTEMBER 2009
Boston, MA
Cincinnati, OH
Los Angeles, CA
Vancouver, BC

OCTOBER 2009
Atlanta, GA
Denver, CO
Edmonton, AB
Ottawa, ON
Washington, DC

NOVEMBER 2009
Chicago, IL
Dallas, TX
San Francisco, CA
Toronto, ON

DECEMBER 2009
New York, NY
Washington, DC

Privacy Certification Exams

SPECIAL NOTES:

Keep your eye on the IAPP Web site and the Daily Dashboard for additional dates and locations to be added throughout the year. Registration opens at least one month prior to the exam date.

For study materials visit www.privacyassociation.org and click “certify.”
Europe debates notifications  
continued from page 8

fines. Richard Thomas, the UK Information Commissioner, is pushing for fines of up to 10 percent of a company’s revenue. As he noted in a recent speech at the RSA Europe conference in London, “the threat and reality of substantial penalties will concentrate minds and act as a real deterrent.”

Interestingly, however, he’s against mandatory data breach notifications. “Put simply, where the risks posed by security breaches are serious, a notification requirement would be too timid. If they are not, it would be excessive.” Furthermore he worries that an overly broad notification rule would result in “breach fatigue” and lead to public apathy.

Flogging, or the scarlett “B”

Some experts, however, argue that Thomas is overlooking the most effective data breach deterrent of them all. “Being forced to tell customers ‘we have screwed you’ with all the attendant press coverage has had a major impact of boards of directors paying attention to security—orders of magnitude more than reporting regimes like Gramm-Leach-Bliley and Sarbanes-Oxley,” notes Gartner Inc. analyst John Pescatore.

Of course if the EU mandates public data breach notifications, the UK will have to get on board. But it wouldn’t happen overnight: after the EU publishes the revised directive—anticipated to occur in mid-2009—member states typically pass national laws which instantiate it about 18–24 months later.

Even if mandatory notifications don’t make it into the directive, however, the legislative writing is on the wall, especially in the UK.”

“Even if mandatory notifications don’t make it into the directive, however, the legislative writing is on the wall, especially in the UK.”

Mathew Schwartz, a freelance journalist based in England, has covered information security issues for more than a decade.