THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
January - February 2011 • Volume 11 • Number 1

Privacy forecast for 2011

At the end of each year, the Privacy Advisor asks a group of global privacy professionals to share what they see in the year ahead for privacy and data protection. In this first issue of 2011, we present their forecasts.

Healthcare Privacy in 2011

By Kirk J. Nahra, CIPP

The big buzz involves whether the HITECH era finally will begin. To date, almost two years since passage of the law, little has changed, beyond the important developments related to security breaches. We have not seen significant new enforcement, despite the opportunities created by the law. And, the Department of Health and Human Services (HHS) continues to struggle with developing appropriate regulations to implement the HITECH law, with a final regulation expected sometime this year. In 2011, we'll finally see the complete package of HITECH regulations – including the conclusion to the debate over notification for security breaches. And, we might see a new enforcement approach—but it's looking more and more likely that any changes will be incremental. The wild card on enforcement—the State Attorneys general who are now empowered to enforce HIPAA—without the knowledge or self-control exhibited to date by HHS.

We're also going to see an ongoing debate about electronic health records. HITECH money will start flowing to providers that implement electronic records. But this may be a make-or-break year for health information exchanges. So far, these are much more expensive and much less valuable than predicted. There will need to be significant progress in 2011—on both industry standards and actual development of working exchanges—before this enormous effort can yield any material benefits.

Kirk Nahra is a partner with Wiley Rein LLP in Washington, DC, where he specializes in healthcare, privacy and information security litigation and counseling. He serves on the Board of Directors of the IAPP and is the editor of Privacy Advisor. *He can be reached at 202.719.7335 or knahra@wileyrein.com.*

Australia and New Zealand: A snapshot of the next 12 months

By John Pane, CIPP, CIPP/IT

Down under, we have started the new year with a bang, but not the type one looks forward to. Vodafone, one of our largest telcos, appears to have suffered Australia's largest ever data breach event. It has been suggested that up to four million customer records may have been compromised. The details include names, home addresses, driver's license numbers and credit card details. Newspaper reports suggest that criminal groups have paid for the private details of some Vodafone customers to blackmail them. Other people were said to have obtained logins to check their spouse's communications. The personal details, accessible via a Web portal, also include numbers dialed or texted plus the time and location of calls or texts.

The full extent of the privacy breach is unknown as investigations by both Vodafone and the Office of the Information Commissioner are still underway. This may be Australia's first "privacy Chernobyl" and the full effects of the event are yet to be felt. I strongly suspect the data breach reporting regime recommended by the Australian Law Reform Commission (ALRC) in its review of the Privacy Act 1988 (Cth), but forming part of the second tranche of proposed legislative change relating to the review of the act, may in fact be brought forward. In my opinion, it absolutely should be.

We also have the prospect of changes to our credit reporting framework, and this change will be largely welcomed, as the relevant section of the Privacy Act 1988 (Cth) under which credit reporting information is regulated is very complex. It is therefore quite difficult to manage from the perspective of both business and the privacy regulator. Simplification of these regulations, without diminishing consumer protection, is greatly welcomed.

As mentioned above, the ALRC recommended that the Commonwealth government repeal the two separate sets of privacy principles regulating the public and private sectors and replacing them with unified "Australian Privacy Principles." It is hoped a bill containing the proposed Australian Privacy Principles will be available later this year. This means it will be a very exciting time for all Aussie privacy professionals, and I look forward to this change with great relish!

"Across the ditch," 2011 also looks to be an exciting new year for our New Zealand colleagues and cohorts. There are many interesting and important developments happening there now, and there are more in the pipeline. Here are a few:

- With support from the Privacy Commissioner's Office, the Privacy (Cross Border) Amendment Bill came before the Select Committee at the beginning of July and was subsequently passed. Passing the bill is a vital step to enable the European Union to deem New Zealand's privacy laws as "adequate" with the EU Directive.
- Developing technologies such as geolocation services
- The evolution of public policy surrounding significant health information privacy issues around the new National Health IT Plan, shared electronic health records and governance of national collections of health information and biological material. The draft National Health IT Plan, released in 2010, is an important step in New Zealand's movement towards devising an effective electronic health records system. As in other countries, New Zealand's health agencies are considering ways in which technology can enhance how health information is managed.

- The New Zealand Law Commission published two major volumes on privacy. The first was the report on Invasion of Privacy: Penalties and Remedies (on reform of such matters as offences and the development of tort law). The second was the issues paper on the Privacy Act itself (Review of the Privacy Act 1993). This could involve a substantial rewrite of New Zealand's privacy laws.
- An amendment has been proposed to the Credit Reporting Privacy Code for public consultation. If the amendment proceeds, among other things, it would allow more comprehensive credit reporting in New Zealand, including reporting "positive" information about people.

John Pane, CIPP, CIPP/IT, is president of the iappANZ.

Report Fallout: A Look at the FTC and Department of Commerce Papers

By Lisa Sotto

The end of 2010 brought a flurry of activity in the U.S. privacy arena. On December 1, the Federal Trade Commission (FTC) issued its long-awaited report on consumer privacy, distilling many of the themes the commission had explored in its series of privacy roundtables. The report, which is intended to inform policymakers and lawmakers, proposes a new "normative framework" for privacy in the U.S. This is indeed a lofty proposition. The document addresses the two main historical themes of U.S. privacy law, i.e., notice and consent and a harms-based model, and it suggests that these paradigms are no longer sufficient to address modern privacy concerns. The commission proposed moving beyond a consideration of monetary damages and tangible harms to intangible injuries such a harm to human dignity. This shift represents a sea change in the way we conceive of injuries in the privacy setting. In addition, the FTC focused in its report on data that can be linked to either a human or a device. This extraordinarily broad scope, coupled with the FTC's skepticism of attempts to anonymize data, means that the set of data elements traditionally considered to comprise "personal information" would be significantly expanded. Finally, the report contains numerous EU-style proposals, such as offering choice at the point of collection, providing access to data and ensuring data integrity. These are relatively foreign concepts to most U.S. businesses.

Following the issuance of the FTC paper, the Department of Commerce put forth its own green paper. Commerce, which had been dormant in the privacy space for a decade, has clearly chosen to reappear on the global privacy stage. The commerce report proposes the development of an updated set of Fair Information Practice Principles. It also recommends that stakeholders collaborate in crafting binding Privacy Codes of Conduct. These bold proposals will make 2011 an exciting year for privacy professionals.

Both the FTC and commerce reports challenge the adequacy of traditional self-regulatory efforts in the United States. Both papers propose a significant overhaul of the country's privacy framework. These reports set the stage for an extensive dialogue within the domestic privacy community. The coming year promises to cast a bright spotlight on privacy and data security in the U.S.

Lisa Sotto is an IAPP board member and partner in the New York office of Hunton & Williams, LLP, where she heads the firm's Privacy and Information Management Practice.

The OPC's Year Ahead

By Jennifer Stoddart

The Parliament of Canada recently approved my re-appointment for a three-year term. I welcomed the invitation to stay on because there are still some important things that I would like to do. I've set a few key priorities:

- Leadership on priority privacy issues. You can expect to see us continue to focus our work in the online realm and on public safety issues, which both have such important impacts on the privacy rights of Canadians.
- Supporting Canadians, organizations and institutions to make informed privacy decisions, and
- Service delivery to Canadians.

While all of the work we do is important, at the end of the day, the priority that is most important to me on a personal level is service to individual Canadians. I want to ensure that people calling my office for help with a problem will receive the level of service they expect from us—whether they are calling about a headline-grabbing issue or more routine types of complaints that don't get any public attention.

Jennifer Stoddart is the privacy commissioner of Canada.

Smart grid privacy developments in 2011

By Rebecca Herold, CIPP

PIAs will emerge as a corporate necessity, with utilities leading the way

As utilities start converting their customers to smart meters and connecting to the smart grid, and as vendors create new types of smart appliances, meters and applications to use within the smart grid, they are going to find themselves faced with a large number of questions asking them to prove that their offerings are secure and protect the privacy of all consumers involved within the homes and personal electric vehicles (PEVs) being integrated within this vast new type of network. As a result of this concern, as well as new federal requirements that will come to pass, we are going to see privacy impact assessments (PIAs) used more within the energy sector and related vendor businesses than we've seen to date in other industries, with the exception of federal agencies. However, the PIAs performed typically will be at a greater depth than those performed to date within the federal offices.

The first thing I did when I started leading the NIST smart grid privacy group in the summer of 2009 was a PIA of the consumer-to-utility portion of the anticipated smart grid architecture. It was the perfect first step; the results clearly revealed where privacy concerns existed. The concepts were transferred to the rest of the smart grid. Since this time the Smart Grid PIA has been referenced and pointed to many times by numerous government oversight agencies, such as the Department of Commerce, Department of Energy, Federal Trade Commission and others, as a model for entities involved with the smart grid to follow. (See it within NISTIR 7628: "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid.") As a result, PIAs are getting more support and are being recommended by more government agencies than at any other time and in any other industry. In the past five

months, not a week has gone by without some entity that is involved, or wants to be involved in the smart grid, that has contacted me asking to get more information about doing PIAs. The year 2011 will be the year that PIAs actually become an activity known by not only privacy professionals, but also by information security, compliance and business leaders alike.

New privacy standards for smart grid entities will be released from the DoC, and/or the DoE, and/or the state PUCs

There has been much push from the utilities throughout the past year to have something solid to follow with regard to standards, rules or regulations for using smart meters, smart appliances and the data that will be created, transmitted and otherwise used within the smart grid. There is much concern on the part of the utilities about how third parties, who have access to smart grid data, will be protecting it. Requirements need to exist for ALL types of entities that possess or have access to energy data, even for those entities that received the data directly from consumers. There is also a growing push from consumers for government agencies to create privacy protections for energy data, and to require entities to establish specific controls for how the smart grid protects personal information as well as information that can reveal personal activities but may not, yet, be considered as "personal data." California has already enacted a smart grid data privacy law, but I expect that, unlike what happened with SB 1386 and the U.S.'s premier breach notice law from California, other states will enact laws and/or regulations that encompass more issues than the California smart grid data law and will not be so much cookie-cutter-copies of the California law. If laws/standards/regulations are not created, advancement of smart grid projects will be significantly reined-in.

Rebecca Herold, The Privacy Professor, is an information privacy, security and compliance consultant, instructor and author who has published 14 books and over 200 articles in her field.

A Big Year Ahead

By Miriam H. Wugmeister

This is going to be a big year for privacy and data security. Privacy is getting attention in a way that we have not seen before. Consider for example the recent articles in The Wall Street Journal and the joint enforcement efforts against companies led by Canada. We are seeing increased activity by legislators, enforcement authorities and politicians all over the world. Whether the attention stays focused on these issues and whether new legislation is passed will depend in large part on the economy and world events, which may shift the focus away from privacy to more pressing issues such as jobs, healthcare and nation building.

In Asia, we may see a new law in the Philippines, and we expect to see continued active enforcement in Korea. We also might see amendments to the laws in Australia.

In Latin America, the new omnibus law in Colombia is likely to be approved by the Constitutional Court and then signed by the president, and we may see a new law in Brazil.

In Europe, the EU Commission is seeking to publish an initial draft of its proposals regarding the revision to the EU Privacy Directive before the summer. We anticipate that data protection requirements will become stricter in Europe, with an increased focus on security and a general breach notification requirement. EU member states are in the process of implementing the ePrivacy Directive, which includes strengthened consent requirements for

cookies and security breach notification for "providers of publicly available electronic communication services," which encompasses ISP and telecommunication operators but in some countries will also include commercial Web site providers. We also are likely to see a significant revision of French data protection law and new rules for employee privacy in Germany.

In the U.S., in addition to the work being done by the Federal Trade Commission and the Department of Commerce, we are likely to see several bills introduced, including by Senators Kerry and Pryor and one by Representative Markey, one of the drafters of COPPA, who intends to introduce a children's privacy bill that will include a do-not-track mechanism for online behavioral advertising to children. This comes at the same time that the FTC is reviewing (and will likely propose changes to) its COPPA rule. While it is unlikely that privacy will get much legislative attention in the House Commerce Committee—a crucial path to any new law's passage—there will surely be a continuation of the types of hearings we have seen in recent years in both the U.S. House of Representatives and U.S. Senate.

All in all, there is a real opportunity for stakeholders to influence policy and to actively participate in shaping the rules, regulations and policy positions for the years to come.

Miriam H. Wugmeister is a partner in the New York offices of Morrison & Foerster LLP.

European outlook

By Eduardo Ustaran

In Europe, it is clear that the review of the 1995 data protection directive will preside over all other privacy-related developments, although data security scandals will almost certainly make quite a few front pages. In all likelihood, the European Commission will take centre stage, mulling over the submissions made by an unprecedented number of interested parties and deciding what legal mechanisms, principles and obligations best meet their twofold policy goal—the defence of the fundamental right to data protection and the flow of personal data within the EU.

However, 2011 will not just be about policy making. In fact, it will not take very long before privacy regulators all over the world start using their brand new (or nearly new) powers—the UK and Poland being prime candidates for flexing their muscles early in the new year.

Early indications also show that regulators in Europe and beyond will continue to target Internet companies and turn their attention to issues like analytics technology, apps and contacts importers. On the cookie front, the truth is that the uncertainty surrounding what qualifies as consent across EU member states will continue throughout the year. However, that deadline may pass almost unnoticed as, at about the same time, the European Commission will publish its concrete proposals for a new data protection regime in the EU, which is likely to become a key focus of attention for international privacy professionals.

Eduardo Ustaran is a partner at Field Fisher Waterhouse in London and is the head of the firm's Privacy and Information Law Group. He is a member of the IAPP Board of Directors.

Reding's Top Priorities

From the office of the EU Justice Commissioner…

Vice-President Reding's top priority for 2011 is the substantial reform of the EU rules on data protection, leading to a modern and comprehensive framework for data protection in the EU. She started working on this at the end of last year, and here you will find more information about the issues at stake: European Commission sets out strategy to strengthen EU data protection rules.

"Since the Data Protection Directive came into force in 1995, our principles have stood the test of time and remain valid. While the directive's core principles remain solid, modern technology and globalisation pose new challenges to data protection. That is why we need to modernise our rules to respond to the challenges of today's information society. These challenges include behavioural advertising, cloud computing and social networks. I am planning to present the new measures this year.

We want, first of all, to strengthen individuals' rights, particularly the right to be properly informed about the way their data is being processed and to be able to access, correct and, where appropriate, have them deleted—everyone should have the "right to be forgotten." This is especially important nowadays given the massive amount of personal data processed on the Internet. We also want to help businesses by reforming the rules and making them more simple and clear. At the moment, a company that operates in several different countries in the EU often has to face different data protection standards. For instance, there may be different ways that data protection authorities interpret the rules. This leads to a lack of clarity about which countries' rules apply, harming the free flow of personal data within the EU and raising costs. Legal certainty is particularly important when data is transferred from one country to another."

—Viviane Reding, European Commission Vice-President, EU Justice Commissioner *Miriam Wugmeister is a partner in the New York offices of Morrison Foerster LLP and is chair of the firm's Global Privacy and Data Security Group.*

The year ahead for Canadian privacy pros

Jeff Green and the privacy team at RBC collaborated on this list of what privacy pros in Canada and beyond will be watching for and/or grappling with in the year ahead.

1. Increased focus in the industry on "data minimization" as a strategy to address privacy concerns.
2. "Privacy by Design" will grow as a buzzword to promote privacy worldwide, but there will not be a common, worldwide definition of what this means.
3. Attempts by regulators to control tracking of Internet activity techniques such as data mining and cookie tracking will be ineffective in 2011.
4. The focus for consumer awareness programs will increase around "privacy" as well as "identity theft" as it becomes necessary to find new ways to reach the consumer.
5. Behaviour-based advertising will continue to be welcomed by a large part of the general public, thwarting attempts to control its use.
6. The Canadian privacy regulators will continue to play a significant role in the worldwide promotion of privacy issues and challenges.

7. Companies and regulators will struggle with the paradigm shift of how information moves and is stored in a world of iPads and Powerbooks.
8. The United States will continue to struggle with a national data protection law, but with the onset of the new consumer protection bureau in financial services, the financial regulatory agencies and the FTC will make advances in data protection regulation.

Jeff Green, CIPP/C, is vice-president of global compliance governance and chief privacy officer at RBC. He is vice-chairman of the IAPP Board of Directors.