Protecting Customers’ Privacy Through Consistent Development Practices

Peter Cullen

As consumers increasingly rely on the Internet for shopping, banking, e-government and other activities, privacy has become both a major public concern and a barrier to the growth of Internet services and online commerce. Widely publicized data breaches, alarming statistics about privacy incidents and fear of identity theft all threaten to erode trust in the Internet. In fact, RSA Security’s 2006 Internet Confidence Index found that nearly half of U.S. consumers have “little or no confidence” that organizations are taking sufficient steps to protect their personal data. At the same time, consumers are more frustrated with software and Web sites that do not clearly communicate the potential impact to their privacy, or do not consistently offer them controls over how their personal information is used.

The software industry can help address these issues by establishing a high bar for respecting customer privacy. However, there are currently no industry-wide prac-
Notes from the Executive Director

The pace of the IAPP’s privacy events and the enormously successful Academy conference in Toronto last month are indicative of the demand in the marketplace for privacy pros and the IAPP’s role as the leading professional organization for our growing global ranks. The IAPP Privacy Academy 2006, our first conference outside the U.S., served as the backdrop for the launch of our new CIPP/C program for Canadian privacy pros. The Toronto conference, which attracted 750 attendees, was our most successful Academy in our 5-year history.

The Academy also gave us an opportunity to recognize some of this past year’s privacy leaders during a memorable member reception held at the Hockey Hall of Fame. Open exclusively for Academy attendees, the Hockey Hall of Fame exuded an aura of greatness and stellar achievement, serving as the perfect setting to recognize the high achievers in our own profession.

I would like to thank Deloitte for sponsoring the IAPP/Deloitte & Touche Vanguard Award, which recognizes the privacy professional of the year. This year’s award was given to a dedicated privacy leader, Chris Zoladz of Marriott, a member of the IAPP Board of Directors who also is the past president. I want to extend my personal congratulations to Chris, who is more than deserving of this recognition for his ongoing contributions to our profession.

Also delivered during a lively presentation in the NHL Legends hall were the IAPP Innovation Awards, given annually to recognize privacy leadership in the public, private and technology sectors. I also would like to recognize the four companies that won this year’s award: Royal Philips Electronics and General Electric Corp., which tied in the Large Organization category; ATB Financial, which won in the Small Organization category; and Voltage IBE, which won the second annual Technology Award.

No sooner were the Toronto boxes unpacked when it was time to crank on the remainder of our whirlwind of fall activity. Most notably, we proudly hosted The IAPP Privacy Dinner in Washington, D.C., which gathered Federal Trade Commission Chairman Deborah Platt Majoras, top CPOs, regulators, attorneys and consultants. The first-ever privacy dinner provided a rare opportunity to network and share a meal with leading members of the privacy community. Held Nov. 6 at The Willard Hotel, the event was a notable complement to the Federal Trade Commission’s Tech-ade hearings.

All the while, we already are deep into the planning stages for the IAPP Privacy Summit 07 in Washington, D.C. The IAPP also will soon announce an exciting initiative to help in our commitment to provide the most relevant and best educational opportunities to our members. I am proud to announce that we will soon unveil the membership of our new Education Advisory Board, which will assist us in developing strong programming for the profession in the months and years ahead.

Thank you for the contributions you make that propel the success of our profession. We will continue to help you thrive in your career as we look to you to fulfill your duty to serve the profession through the IAPP.

J. Trevor Hughes, CIPP
Executive Director, IAPP
Secure Webmail 101 continued from page 1

first thing that comes to mind?
If you’re like most people, you might think about an employee accidentally sending out an email containing sensitive information about its customers or employees — and in the blink of an eye — the company is faced with an unwanted disclosure affecting thousands of people. Or you might think about an employee hitting reply-all to a particular message instead of reply, and thereby exposing sensitive information to a much wider audience than intended or permitted by the corporate policy. You might ask, just how frequent are email errors made by an organization’s own staff?

Frequent enough. According to The New York Sun (Oct. 11, 2006), just last month, a political staff member accidentally addressed an email containing a list of some of the party’s top donors, along with their Social Security numbers, dates of birth, and race. As a result, it found its way into a Gmail Web-based email account and the media had a frenzy over why such information was being sent unprotected within email. As referenced by the Privacy Rights Clearinghouse (www.privacyrights.org), in July, the personal information of more than 8,000 of New York City’s homeless was leaked accidentally in an email. In April, the University of South Carolina reported that the Social Security numbers of as many as 1,400 students were mistakenly emailed to classmates when an employee attached a database file to an email. And, back in February, Blue-Cross, Blue Shield of Florida experienced a breach when one of its contractors emailed names and Social Security numbers of approximately 27,000 current and former employees, vendors and contractors to his home computer, violating a company policy — just six months after the company experienced a similar disclosure via direct mail.

The Many Faces of Email Breach

When it comes to communicating electronically with consumers, there are many ways for a breach to occur. User error, as in the employee misuse cases described above, is not the only source of worry.

Combating Phishing Emails

Phishing is one of the most common ways in which hackers attempt to gain unauthorized access to online banking or other types of user accounts. The hacker sends a consumer a fake, ‘spoofed’ email that appears to be coming from the service provider (such as a bank), asking for the input of personal account information. The unassuming consumer may not realize the email has not actually been sent from his or her bank. In this case, it’s not the user who provides the threat of breach, but rather, the hacker. The bank needs a mutual way of sending a secured email to the consumer to convince him or her of the bank’s integrity, as well as a way for the consumer to securely reply back to the bank. But how can the bank do this when it doesn’t know what kind of email application the user has installed on his or her home PC, or whether the application will be able to accept encrypted emails? The bank certainly doesn’t want to have to train the user to install and manage a personal digital certificate to decrypt, read and reply to emails from the bank. Though this method of “one-off” email encryption has been around for a long time, it has really only been adopted by the most technical email users, such as consultants and those working directly in the IT field.

“Much attention has been paid to protecting consumers through stronger authentication and data security, but what about via email?”

See Secure Webmail 101, page 4
Secure Webmail 101
continued from page 3

Protecting Against the Unsolicited Sensitive Customer Request

Many retailers offer online shopping services with a proper shopping cart transaction system protected via Secure Sockets Layer (SSL) security, so credit card data is encrypted as it is submitted by customers for processing. However, what about protecting against consumers voluntarily emailing customer support team with specific requests pertaining to account details, or worse yet, submitting an order manually and sending credit card data to a consumer in an unprotected email? Consumers likely have encountered several Web sites with an infamous disclaimer posted saying things like the following: “Please do not include any confidential information in your message (such as account numbers or credit card numbers),” or “No messages containing requests about your personal account information will be dealt with via email.” However, experience shows that it’s inevitable that customers will send emails containing this sensitive data. By offering users a secure way to send and receive email communications, organizations will be encouraging customers to do business in the way they feel most comfortable, while putting an automatic measure in place to protect the company’s brand from a potential leakage. Secure email can give customers choice, without compromising their security.

The Value of Protecting Emails for Consumers

Consumers are not restricted to one particular email technology, application, or even Web browser. Not wanting to force users to download and install any specific applications, institutions that need to communicate securely with their consumers are usually limited to direct mail, which is not only costly, but also slow and one-directional. Consumers are demanding real-time service, and enabling electronic communication with them provides the best solution, but at what potential cost to the organization?

Secured email can provide not only peace of mind for privacy protection, but also productivity enhancement, by enabling organizations to move more sensitive and higher value transactions online, as well as enabling electronic delivery of regular communications with customers (such as billing and account statements, insurance claims and application processing documents).

Messages that were previously limited to more traditional methods of communication, because of concerns about information security, can now be moved online with a similar level of assurance of confidentiality as before. However, in order to take advantage of the benefits of online communication with consumers, security and trust are essential.

Consumer Email Security Gaining Momentum

The “lowest common denominator” of online consumer security is SSL-protected Web sites. SSL security is often verified by a site seal placed prominently in view on the service provider’s Web site to let consumers know the site can be trusted for secure transaction processing. Though all providers of credible online services such as banks and retailers have SSL security deployed on their Web sites, not many offer secure email.

But that is changing. Citibank, plagued by the threat of phishing, has risen to the security challenge by offering its registered users an online secure mailbox which they can utilize to communicate with the bank. As part of Citibank’s online security practices described on its Web site (web.da-us.citibank.com), Citibank will notify users by email when there is a message waiting for them in the online inbox, and the email sent can be verified using something they refer to as the “Email Security Zone” containing the user’s first and last name, and the last four digits of their ATM/debit card.

Protecting Email for Your Consumer Base: Secure Webmail to the Rescue

Powered by a gateway or boundary email server placed at the edge of a company’s network, email messages coming from a typical enterprise mail client, such as Microsoft Outlook, can now be encrypted for mass consumer users, without knowing what kind of email application they are using to access their messages. This can be achieved using a boundary email security solution that supports secure Web-enabled mail delivery.

Boundary Email Security

Boundary email security solutions are easier to install and manage since they do not require that client software be installed on user desktops. Senders need not worry about manually choosing to encrypt or not encrypt a message for a particular user, as the server does that for them. When setting up the boundary solution, the company can set policies for encrypting messages automatically before they leave the corporate network, such as “encrypt all messages,” or “encrypt all messages going to a certain type of domain,” or “encrypt all messages coming from a particular set of users.” This automation means an organization doesn’t have to worry about a potential email disclosure of sensitive information because all messages will be encrypted without relying on users to take any specific action.

“The list is long and the possibilities are wide for how Secure Web-enabled mail for consumers can help transform the online world into one of trust as well as one of greater efficiency.”
Secure Web-enabled systems use SSL-based protocols in the delivery of secured messages. There are two primary models for secure Web mail message delivery — pull and push. Within pull models, a notification message along with a URL, is sent to the recipient to pull the user back to a Web portal where a secure inbox is displayed. The recipient can then view the secured message using a common browser authenticated via an SSL session. According to Gartner, “Secure email solutions using a ‘pull’ approach are best for business-to-consumer (B2C) communications.” (Gartner “Differentiators of Leading Secure E-Mail Architectures”, Eric Ouellet, Feb. 28, 2006) Within push models, a secured message is delivered to a recipient, pushed as an attachment along with executable code, for users to decrypt and display the message directly in their Web browsers. Decryption keys for the push methodology are managed by the sending organization and delivered to recipients through an authenticated SSL connection.

A good boundary email solution is one that enables flexibility in the delivery of encrypted messages. It will do the heavy lifting for the sender, by determining which delivery format is required for each particular recipient, based on their domain, and deliver it accordingly — in other words, users of Web-based email services such as Hotmail and Yahoo! will be pushed or pulled to access secure messages via the Web-enabled delivery method, while users with mail clients that support traditional encrypted email formats such as SMTP or PGP, will be able to read and reply to the messages within their existing mail clients. This integration with pre-existing email security systems such as those driven by Public Key Infrastructure solutions, and transparency to users, are both critical factors for a successful secure email deployment.

Who Can Benefit From Secure Web Mail?

Banks. Insurance Companies. Healthcare providers. Utilities such as gas, electric and water service providers. Telephone and cable companies. ISPs. The list is long and the possibilities are wide for how Secure Web-enabled mail for consumers can help transform the online world into one of trust as well as one of greater efficiency.

Sealing the Electronic Envelope: Things to Consider

So, if a company could benefit from communicating securely with its consumer base, boundary email security could be the answer. However, it’s important to keep the following in mind. Email security has to be three things for users (and consumers, in particular) to adopt: easy to use, confidence-inspiring and rewarding. It should not require a user to make any more effort to send a secured email than is required to send a regular email, and the communication method itself should reassure the customer that the system is secure and can be trusted to protect his or her personal identity. Lastly, the process of sending and receiving secure emails with the service provider should offer the consumer some value or reward for doing so, be it time or cost savings from doing things online that the user would not have otherwise been able to do, such as file and submit an insurance claim or request changes to their monthly mortgage payments. Secure Web mail can open the door to a stronger customer relationship, and help close the door to fraud.

Privacy Through Consistency continued from page 1

tics to help standardize the user experience for privacy-oriented software features, or to address privacy issues and concerns in the software development process. To help establish a starting point for these efforts and open an industry dialogue about privacy guidelines for development, Microsoft has released an extensive set of public privacy guidelines for developing software products, Web sites and services. These guidelines draw from the company’s experience incorporating privacy into its development processes and address customers’ expectations about privacy as well as privacy legislation in effect worldwide. For example, they reflect the core concepts of the Organization for Economic Cooperation and Development (OECD)’s Fair Information Practices and privacy laws such as the European Union Data Protection Directive, the Children’s Online Privacy Protection Act of 1998 (COPPA), and the Computer Fraud and Abuse Act.

The Privacy Guidelines for Developing Software Products and Services can be found in the “Related Links” section of www.microsoft.com/privacy.

Privacy concerns are easy to understand in principle, but challenging to address in practice, particularly in the development of software. Similar guidelines have helped Microsoft’s developers to better understand and address privacy issues. Our hope is releasing a public version of the guidelines can promote an ongoing industry dialogue on protecting privacy through consistent development practices.

The public Privacy Guidelines for Developing Software Products and Services are based on the internal privacy practices incorporated in the Microsoft Security Development Lifecycle (SDL), a process that helps ensure that the company’s products and services are built from the ground up with security and privacy in mind. The SDL implements a rigorous process of

Steve Duncan is a Senior Product Manager with Entrust. With more than 20 years of experience in technology marketing and sales, Duncan is responsible for driving the Information Protection Security Solutions portfolio at Entrust. He and his team are focused on creating a well integrated portfolio of solutions designed to protect customer’s intellectual property and sensitive information. Duncan can be reached at +613.270.3406 or by email at steve.duncan@entrust.com.
Privacy Through Consistency
continued from page 5

secure design, coding, testing, review and response for all Microsoft products deployed in an enterprise, that are routinely used to handle sensitive or personal information, or that regularly communicate via the Internet.

The guidelines cover a wide range of topics, including:

• Definitions of different types of customer data, including personally identifiable information (PII) such as the user’s name and email address, sensitive PII such as credit card or Social Security numbers, and anonymous or pseudonymous data.

• Guidelines and sample mechanisms for notifying users that their personal data may be collected, and offering them ways to consent (or not) to the collection of this data.

• Guidelines for making disclosures to the users about how their personal information may be used.

• Reasonable steps to protect PII from loss, misuse or unauthorized access, including access controls, encryption, physical security, disaster recovery and auditing.

• Control mechanisms for users to express their privacy preferences, taking into account the needs of system administrators, as well as special guidelines for shared computers.

• Strategies to prevent data leakage by minimizing the amount of personal information that needs to be collected.

To set the proper foundation, the first half of the guidelines is devoted to general concepts and definitions. The second half lays out specific rules for common scenarios that can affect a customer’s privacy, such as transferring PII to and from the customer’s system, installing and updating software on the customer’s system, storing and processing customer data over the Internet, and transferring customer data to third parties. The guidelines also provide additional requirements for deploying Web sites, for software targeted or attractive to children, and for server products within an enterprise (including measures to help system administrators protect the privacy of their end users).

One example scenario covers the development and policy guidelines for deploying a public Web site. According to the guidelines, the site must provide a link to a company-approved privacy statement on every page, regardless of whether PII is collected on that page. The link should not be smaller than other links on the page, such as legal notices, and it should be in a consistent location, such as the page footer. This rule also applies to pop-up windows that collect PII. For lengthy or complex privacy statements, the site should adopt a “layered notice” format, which includes a single-page summary of the statement that provides links to more detail. Additionally, the privacy statement should be compliant with the Platform for Privacy Preferences (P3P) standards for machine-readable statements, and, if appropriate, certified by an independent organization such as TRUSTe.

The site also should avoid the unnecessary use of persistent cookies when a session cookie, which is retained only for the duration of the browser session, would be adequate. When using persistent cookies that store PII, the site should get explicit consent from the user and store the PII in an encrypted form. If a site collects any form of PII from the user, it must adhere to specific guidelines for notice and consent, security and data integrity, and customer access and control. If it stores persistent data on the customer’s system, in cookies or any other form, it must adhere to a number of additional guidelines, including appropriate user notice and consent for storing PII, using encryption where relevant and other methods that help secure data in storage such as file permissions, as well as a consistent means to give users the opportunity to view and delete their PII, or prevent it from being stored at all.

Finally, if the site is directed at children, it should adhere to even stricter guidelines across the board, to empower parents to supervise and control their children’s browsing experience as well as comply with legislation such as COPPA.

For several years, a number of product groups at Microsoft have been following similar privacy guidelines as part of the SDL. For example, development of the recently released Microsoft Phishing Filter included a number of key design decisions to help reduce the impact on our customers’ privacy, including not storing IP addresses with the other data collected by the Phishing Filter (Web site addresses to be checked) to avoid potential correlation. Other decisions included having the Phishing Filter only send the domain and path of the Web sites to Microsoft (removing search terms) and sending the Web site addresses to Microsoft via SSL. We invited Jefferson Wells, an independent third-party auditor, to run two separate audits on the technology, which validated and confirmed our claims regarding how we handle customer data with the service.

Similarly, when customers run the current version of Windows Media Player for the first time, their privacy experience directly reflects our internal

See Privacy Through Consistency, page 20
Ann E. Donlan

The IAPP Privacy Academy 2006 in Toronto served as the debut for the IAPP’s new certification credential, the CIPP/C, the first professional credential for Canadian privacy professionals, and showcased the IAPP’s commitment to serve its domestic and international members with educational content tailored for Canada’s privacy scheme and laws.

Privacy professionals from across Canada and around the world gathered last month for four days of lively panel discussions, networking forums, working groups and featured keynotes from top policy makers and corporate leaders in the privacy industry.

Canadian privacy officials, including Privacy Commissioner Jennifer Stoddart, raised the profile of the event even more with their keynotes during the IAPP’s three-day event at Toronto’s Westin Harbour Castle, on the scenic shores of Lake Ontario. The Canadian media, including Canada’s cable news channel, CTV NEWSNET, covered the Academy and newsworthy announcements made during the event. Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, held a news conference at the Academy with Microsoft to announce the 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age. In addition, Microsoft released The Privacy Guidelines for Developing Software Products and Services, an extensive set of privacy guidelines for developing software products, Web sites and services, which coincided with an Academy panel on the closing day, “Privacy in Product Development.”

Attendees count on the IAPP to foster effective networking events to help them connect with their peers, research career opportunities and have fun with fellow privacy pros. The Academy offered attendees a selection of networking venues — everything from the small, informal dinner with fellow privacy pros in specific industries to an exclusive reception at Toronto’s venerable Hockey Hall of Fame — even a competition to test the networking prowess of attendees for the title of king or queen of networking. The networking dinners — a new, but popular way of connecting with peers — was a welcome addition to the offerings.

“I thought the sign-up dinners were a phenomenal addition to the overall experience,” remarked one happy participant.

CIPP, CIPP/G, CIPP/C Trainings, Preconference Sessions Kick Off Academy

Before the Academy was in full swing, students participating in the Oct. 17 trainings for CIPP/C, Part I, and CIPP/G training, were intensely preparing for their examinations, scheduled later in the week. Bright and early the next day, CIPP/C training continued for those students taking Part II. A separate class devoted the entire day to training for the CIPP exam.

While students were focused on exam preparations, attendees eager for in-depth training on particular topics, including the ever-popular Privacy Professional Bootcamp, spent the afternoon engrossed in Preconference Sessions. Besides the bootcamp, Preconference Sessions were held on Payment Card Industry (PCI) Data Security Standard — A Workshop; RIM Council: An Introduction to the Responsible Information Management Framework; and Outsourcing and Trans-Border Data Flows: Privacy and Public Policy in Transition.

That evening, the invite-only Speaker Dinner, sponsored by PricewaterhouseCoopers, gave guests and dignitaries the chance to mingle at Downtown Toronto’s Far Niente, where they enjoyed a salmon dinner, featuring a delectable dessert.

See IAPP Toronto Conference, page 8
Day One: Opening Plenary, Break-Out Sessions, Chopper in the Exhibit Hall

IAPP Board President Kirk M. Herath, CIPP/G, welcomed more than 750 attendees who jammed the Westin Harbour Castle’s Metro Ballroom for the Opening Session and Keynotes.

Herath was followed by IAPP Executive Director J. Trevor Hughes, an Ontario native and CIPP, who said he was the IAPP’s second largest of the IAPP’s more than 20 networking groups.

Hughes revealed for the first time publicly that the IAPP is planning to expand its certification programs by offering credentials in other parts of the world. The success in the marketplace of the IAPP’s certification programs is evident in the sheer number of graduates who have successfully passed the CIPP exam — 1,000 in the two years since the program’s launch.

“We are certainly building a profession,” Hughes told attendees. “And there are many of us doing that building right now,” added Hughes, who noted that the IAPP membership has grown to 2,800 members in 23 countries.

Hughes elaborated on the critical role of today’s privacy professionals. “There is a need for guardians of trust — for guardians of that data,” he said. “I’d like to suggest that we are those guardians, that we are those guardians of the information economy.”

In his concluding remarks, Hughes stressed the role of leadership in serving as guardians of the data. “The risks associated with the information economy create a real need for leaders.”

Ontario’s Privacy Commissioner Explains Need for ‘Single Identity Metasystem’

Dr. Cavoukian then used her plenary remarks as a platform to build upon her public announcement the day before. During a well-covered news conference, Cavoukian — joined by Kim Cameron, Chief Identity Architect, and Peter Cullen, CIPP, Chief Privacy Strategist, both of Microsoft Corp. — explained to the media the genesis of the 7 Laws of Identity, which Cavoukian touted as a tool to “profoundly shape the architecture and growth of a universal, interoperable identity system needed to enable the Internet to evolve to the next level of trust and capability.”

In her prelude to her plenary PowerPoint presentation, Cavoukian said e-commerce is in “a state of crisis,” which prompted the need for a system that will reduce online fraud, help to verify online identities and foster trust among users who are increasingly wary of conducting business online.

“Online fraud is growing at an alarming rate,” Cavoukian told the crowd. “…Companies’ reputations and brands are being impacted dramatically by these deceptive online practices.”

Improved user control is the answer, Cavoukian said. “The growing identification requirements on the Internet are posing enormous privacy problems,” she said. “Trust is at an all-time low.”

Cavoukian added, “The future of privacy revolves around identity, so what can we do?”

Cavoukian described her plan, developed through Cameron’s leadership, as “a single identity metasystem … that empowers users to manage their own digital identities.” (More information is available at www.ipc.on.ca)

In her concluding remarks, Cavoukian warned, “There never has been a more strategic time to ensure that privacy interests are built onto the new architecture of identity.”

Author Don Tapscott: ‘This Ain’t Your Father’s Internet’

Tapscott took attendees on a tour of the Internet, a journey he said is no
longer “your father’s Internet.” Demonstrating Web sites that create online profiles of users — some of which may be inaccurate — Tapscott led attendees to various sites to demonstrate the trail of “digital crumbs” left by users as they surf the Web.

“These sites and capabilities are not necessarily bad,” he said. “They just pose a huge challenge for us as individuals. The sites ‘can collect dossiers of each of us which are beyond the capabilities of any secret police in history.”

Tapscott described a “fundamental change in the nature and capability of the Internet” on a number of fronts, with “billions and trillions of inert objects in our world that (have) become smart communication devices.”

Doorknobs. House keys. Toasters. Dishwashers. “All of this stuff talks to itself,” Tapscott joked. “In five years the shirt will be talking to the washing machine.”

On a more serious note, he continued, “The physical world is becoming smart and inter-connected, and this is a really big change. Now all of these things have something called an IP address.”

Another change is mobility — and the ability to track individuals, whether it be children, friends, celebrities or criminals.

After a demonstration of a number of Web sites to prove his mobility point, Tapscott focused on the profound changes in the Internet’s next generation.

“What is happening is that the Web is changing from a medium to present information to becoming a giant computer,” he said. “When you go onto the Web and you do anything, you are reprogramming this giant global computer.”

Deliberate attempts to falsify an individual’s information and inaccurate information can damage reputations, Tapscott said, as he demonstrated some sites that allow users to post personal information about professors or past lovers.

Tapscott concluded his remarks with a warning about “digital conglomerates” of Internet companies that really up the ante “with the whole question of what we do with information — not just corporate information, but personal information.”

The author of the soon-to-be released book, Wikinomics: How Mass Collaboration Changes Everything, said as companies become more inter-connected and global, they share all types of information. He urged companies to embrace transparency, which he described as “a force in the economy.” He added, “Fitness is no longer an option. If you’re going to be naked, you better be buff!” Values have to be built into an organization’s DNA, he said. “When you open up with customers, you build trust,” Tapscott said.

Tapscott then wound up his remarks with an inspirational challenge for privacy pros.

Privacy, he said, once used to be “on the sideline of corporate strategy. There’s a fundamental change. Privacy is coming into the heart of business strategy. … It’s a leadership opportunity for you. Companies that take the old route, the future is going to be bleak. There’s a new route. As a profession, you did what was possible and you saw the storm clouds and you got organized. But now it’s possible to go forward. The time has come for us to get a grip with this issue. The time has come for each of you to find the leader in you to help your companies do the right thing.”

The IAPP’s Assistant Director, Peter Kosmala, CIPP, then told attendees before the refreshment break in the Exhibit Hall that the number of people at the plenary was the largest Academy attendance in the IAPP’s five-year history.

**Wildside Chopper in the Hall**

All revved up from the inspiring keynotes and the first hour of Breakout Sessions, attendees then shared a networking lunch, which also offered the opportunity to admire Privacy Engineering’s 2006 Wildside Chopper, parked in the Exhibit Hall, which served as a prop for a giveaway.

However, there was a catch. The winner who had the random key to start the stunning bike did not drive away into the Toronto sunset with a brand new $50,000 custom Canadian chopper. The holder of the key to turn over the bike’s engine won a different kind of ride into the sunset — a trip to the Bahamas. The winner was Symantec’s Constantine Karbaliotis, who rattled more than a few attendees when his key started up the thundering machine — inside the Exhibit Hall. Congratulations Constantine!

**Privacy Awards Given During Memorable Hockey Hall of Fame Reception**

After the afternoon Breakout Sessions, the crown jewel of networking events, the Networking Reception, was held at Toronto’s revered Hockey Hall of Fame. During an exclusive event memorable for its delicious h’ors doeuvres and the opportunity to take a slapshot or don the gear of a NHL goalie, attendees wandered around the Hall to view the memorabilia of hockey’s greatest, eventually making their way to the pinnacle display, the awe-inspiring Stanley Cup.

Attendees of the IAPP’s Networking Reception at Toronto’s Hockey Hall of Fame mingle and take in hockey’s legends and storied hockey teams.

Constantine Karbaliotis of Symantec poses with Privacy Engineering’s 2006 Wildside Chopper, after he randomly receives a key to start the monster hog. Karbaliotis won a trip to the Bahamas.
What better way to recognize the privacy profession’s 2006 award winners than to hold the ceremony in the NHL Zone for honored members. Accented in polished black granite and stainless steel, the NHL Zone was the perfect venue for privacy pros to recognize their own distinguished members.

The ceremony honored the winner of the IAPP/Deloitte & Touche Vanguard Award, which recognizes the privacy professional of the year, and the recipients of the IAPP Privacy Innovation Awards, an annual recognition of privacy leadership in the public, private and technology sectors. (See page 14 for more coverage.)

In the Large Organization category (more than 5,000 employees), Royal Philips Electronics and General Electric Corp. tied for their entries on Binding Corporate Rules (BCR) as a mode of compliance for cross-border data transfers.

The winner in the Small Organization category (less than 5,000 employees), was ATB Financial, which won the award for its privacy program communications plan.

Now in its second year, the IAPP Privacy Innovation Technology Award went to Voltage Security, Inc., for Voltage Identity-Based Encryption™ technology incorporated into its data protection solutions.

The 2006 recipient of the IAPP/Deloitte & Touche Vanguard Award was Chris Zoladz, CIPP, Vice President, Information Protection, Marriott International.

Day 2: Three Exams, Working Groups, Closing Plenary, Encore Sessions

The morning of Oct. 20 was tense as nervous examinees prepared to take the CIPP, CIPP/G and CIPP/C tests. By day’s end, 175 examinees sat for all three IAPP credentialing exams in the Frontenac Ballroom.

For others, the Friday Working Groups provided an opportunity to network in their area of expertise: Financial Services; Consumer Marketing; International; Human Resources; Government; Healthcare/Pharma; and Higher Education.

A two-hour seated lunch in the Metro Ballroom then set the stage for the Closing Plenary, featuring Dan Fortin, President, IBM Canada; Dr. Larry Ponemon, Chairman and Founder of The Ponemon Institute; Dr. Eric Johnson, Norman Eig Professor of Business, Columbia University; and Dr. Martha Rogers, Founding Partner, Peppers & Rogers Group.

Big Blue’s Commitment to Privacy

Fortin detailed some of the structural changes IBM has made to accommodate advances in technology. “Our professional services businesses used to have multiple teams in regions,” Fortin said. “Today we manage it as one asset.
The work can be moved around, not tied to a local market.”

He also discussed the prevalence of outsourcing, which Fortin says allows companies to specialize in one area that sets them apart in the marketplace. “Corporations are moving work based on expertise,” Fortin explained.

Fortin touted IBM’s commitment to privacy, noting that it was the first corporation to implement global privacy policies in the 1960s. Last year, the company revised its policies to prevent the use of genetic testing results in personnel decisions.

“Most importantly, you as privacy professionals are vital to issues like trust,” Fortin said. It is essential that customers will receive a “consistent and quality experience time and time again,” which springs from trust, he added.

The 2006 Salary Survey Results

Dr. Ponemon gave a presentation on the results of the 2006 salary survey, which found that while there have been “salary increases in almost every area,” a gender gap remains, although it is less than when measured four years ago.

“But we have a ways to go as a profession,” Ponemon acknowledged.

IAPP certification is a proven way to boost a privacy pro’s salary, Ponemon said.

“CIPPs earn more money,” Ponemon said.

Ninety percent of the survey’s respondents were from the U.S., but Ponemon said he expects to “see more and more non-U.S. respondents as the IAPP seeks to become more international.”

Professor Johnson Captivates Audience — Fire Alarm Sounds, But No One Moves

Johnson started his presentation with a provocative question: “How do people make decisions about privacy?” His answer: “They don’t.”

Much of his presentation — which was interrupted at least twice by an announcement about a fire alarm that ultimately turned out to be false — focused on decision-making and defaults.

“People have strong preferences but they don’t think about those preferences as they conduct their lives,” Johnson said. “A default is what happens when there is an opportunity for you to make an active decision and you don’t. Most privacy decisions have a default option.”

Johnson stressed that “defaults have a big effect on privacy and commerce,” and he urged the audience to study the issue and use the knowledge wisely.

Dr. Rogers Thrills the Audience with Engaging Style, Captivating Message

Dr. Rogers closed the plenary session with a lively presentation that impressed many attendees.

Rogers talked about her company’s Return On Customer strategy, and using privacy as a company growth strategy.

“All of our revenue comes from the customers that we have today and the ones that we will have tomorrow — and that’s it,” Rogers said. “That’s the only chance we have at growing our companies as well.”

Rogers said companies must embrace the concept of “the potential value of our customers tomorrow” as a way to hold managers accountable for their performance.

Companies are limiting their growth by “operating on the false premise” that the manufacture of more products, or offering more services, is the way to make more money. “There’s one thing we can’t make more of. … The one thing that is in short supply for every company, the one thing that limits our companies, is paying customers. We can clone sheep, but we can’t make another human being that is ready and willing to buy our products.”

The key, she said, is to look at achieving the “greatest return on customers.”

See IAPP Toronto Conference, page 15
As with many business environments, direct marketing thrives on customer trust. Maybe customers don’t always know why they trust a business — the products are better, or more reliable, or they feel more secure — but customer trust helps drive long term profitable relationships. One element of trust that we’re hearing more about these days, especially as the promise of ‘personalized’ marketing develops, is how information is collected and used. And with such increasing information use comes an increased set of privacy-related challenges, issues — and yes, opportunities.

As much as customer privacy gets talked about these days, what do marketers think about privacy concepts? There's probably not one concise answer to this question. But a couple of recently released studies help to shed light on how some companies are approaching customer privacy.

Increased Collection

A key component of customer privacy is the idea of providing customers notice and choice about your data practices. At the end of August, the Customer Respect Group, a Massachusetts-based research firm, released the results of its Third Quarter 2006 Online Customer Respect Study of Retailers. The report detailed how online retailers stacked up when it came to privacy, communication, and marketing to their customers.

While the Customer Respect Study found that online retailers are improving their efforts to effectively communicate with customers, it also noted an increase in the types and amount of collected data. More than a quarter of online retail sites, the Customer Respect Group found, required customers to log in or register before they are allowed to view products or prices. And 20 percent of the companies surveyed required customers to provide more than 10 different pieces of information about themselves — such as addresses, phone numbers, and so on — when submitting a question.

As we all know, information is a key ingredient in most effective marketing outreach programs. Unfortunately, the report found that some online retailers did not consistently ask their customers' permission before using collected data for marketing purposes. Of the companies surveyed, 15 percent used collected customer data for internal marketing without explicit authorization — and 43 percent shared such data with business partners or other third parties without first getting explicit customer permission.

A Hindrance to Marketing?

As we all know, information is a key ingredient in most effective marketing outreach programs. Unfortunately, the report found that some online retailers did not consistently ask their customers’ permission before using collected data for marketing purposes. Of the companies surveyed, 15 percent used collected customer data for internal marketing without explicit authorization — and 43 percent shared such data with business partners or other third parties without first getting explicit customer permission.

Privacy as Boon, Not Burden

Marketers and privacy professionals agree, then — customer trust is good, and so is using data to build that trust. Where they diverge, it seems, is how to best use collected data to develop trust. But I think both groups can learn something from each other. Marketing professionals are right to recognize the value of customer trust — and customers certainly respond positively to personalized marketing.

On the other hand, this isn’t the...
only reason customers have to trust a business. There’s also the question about what happens to information once it’s been collected. As Forrester Research has reported, 86 percent of consumers are worried about providing their information to marketers because of privacy and security concerns. Such fears can be a real impediment to customer trust and loyalty.

But the right privacy policies can help alleviate this barrier. “Too many companies fail to understand the strategic significance of privacy within the context of a successful, profitable marketing campaign,” said Dr. Larry Ponemon of The Ponemon Institute. “Privacy is still regarded as an inconvenience to the marketing community, rather than an opportunity to build strong, long-lasting relationships.”

In a forthcoming white paper, edited by Chapell & Associates, The Ponemon Institute’s Responsible Information Management Council will outline how businesses can effectively institute customer privacy to further their marketing initiatives. In this paper and elsewhere, what is clear is that respecting a customer’s privacy leads to increased loyalty and trust. Applied properly, that trust can provide a significant competitive advantage.

**Alan Chapell, CIPP, is president of Chapell & Associates, a consulting firm that helps direct marketers navigate the waters of consumer privacy and develop responsible and effective marketing programs. Chapell has been instrumental in the development of emerging best practice standards for privacy and interactive marketing. He may be reached at +212.675.1270, or via email at achapell@chapellassociates.com.**

---

**Networking Central**

**Billy J. Spears, M.B.A., CIPP/G, and Senior Manager, Privacy & Information Protection, Dell, Inc., will author a new networking feature that will showcase the art of networking — IAPP-style! Look for Spears’ occasional features, based on real-life experiences of IAPP members at networking events.**

**IAPP Networking ... Does it Really Work?**

In this business, we all seem to work flawlessly in our own separate worlds. The majority of our interactions, socializations and communications are through electronic means, such as email or telephone calls. We live in a fast-paced environment where issues swirl over our heads like a tornado waiting to make its first contact with the ground. If it weren’t for events that draw us into the same room, we would never have a face that matches anyone’s emails or voices.

This year at the IAPP Privacy Academy 2006 in Toronto, I experienced a memorable networking interaction with a person I had only talked to through electronic means before this conference. Let me set the scene for you...

I was attending The Privacy Advisor’s networking reception and had just ordered a drink when a woman came up and introduced herself to me. I reciprocated by introducing myself and we shook hands as if it were the first time we had ever spoke. Almost immediately, this woman began asking me questions about why I was not submitting more articles to publish in the Advisor. For whatever reason, I did not hear her name, but I knew I had submitted articles to the editor on several occasions. All I heard was that I wasn’t submitting enough copy so …

I responded to this woman by telling her that I had submitted articles to the managing editor of The Privacy Advisor, Ann Donlan, and she would not push my articles through to print. I also stated that I did not understand why she would not publish them and that she must hate me or something. I am serious as a heart attack. Can any of you guess who I was speaking with? Ladies and Gentlemen, I was face to face with none other than Ann Donlan herself. As she and I cleared up the identity and technical issues surrounding my article submissions, we had a great laugh together and have become even better friends. Ann does not hate me and does not have a grudge against my articles.

The moral of the story here is that networking works. It is evident by the relationships we all have made through our interactions with the IAPP. There are more than 1,000 CIPPs worldwide and the numbers are growing stronger. You should be making contacts and networking with as many professionals as you can. You never know who you are talking to unless you get their name first.

*The views expressed are Spears’ and not necessarily those of Dell, Inc. Spears is a member of The Privacy Advisor’s Advisory Board.*

Managing Editor’s Note: IAPP Members will note that Billy Spears can no longer claim that the Managing Editor blocks his Advisor submissions.
IAPP In The News

IAPP Innovation Award Winners, Privacy Leader of The Year Receive Trophies at Toronto’s Hockey Hall of Fame

The IAPP Privacy Innovation Awards and the IAPP/Deloitte & Touche Vanguard Award were presented Oct. 19 during an exclusive member reception at the Hockey Hall of Fame in Toronto.

More than 30 individual organizations participated in the 2006 Innovation Awards, the largest number of nominees ever in the four-year history of this distinguished awards program.

“"We are delighted to recognize these organizations for their leadership in the development and delivery of privacy programs," said J. Trevor Hughes, Executive Director of the IAPP. "The depth and breadth of nominations this year is a testament to the continued growth of our field.”

Large Organization category (More than 5,000 employees)
This award was presented jointly to Royal Philips Electronics and General Electric Corp., which tied for their entries on Binding Corporate Rules (BCR) as a mode of compliance for cross-border data transfers.

General Electric is the first company in the world to pursue a BCR policy that assures employees that their data will be handled using the highest and best practices no matter where in the world the employee or the data is located. The GE BCR has been approved in more than a dozen countries to date — more than any other model — and is under consideration in all EU countries. This BCR model governs the company’s relationship with its 350,000 employees worldwide and is available in 27 languages.

Philips publicly announced its BCR project at the International Data Protection Conference in Sydney in 2003, when it was already in an advanced drafting stage. The Philips Privacy Code is currently moving through the final approval process in 22 European countries. The unique approach taken by the Philips Privacy Code is that it combines two existing concepts of European data privacy law: the U.S./EU Safe Harbor Program and the (sectoral) Codes of Conduct. The Philips Privacy Code is a self-regulating document which, after endorsement by European Data Protection Authorities, creates a “safe haven” for personal data within the worldwide Philips group.

Small Organization category (Less than 5,000 employees)
The winner in this category was ATB Financial, which won the award for its privacy program communications plan. Alberta, Canada-based ATB Financial is a full service financial institution that is the largest deposit-taking institution headquartered in Western Canada. ATB Financial’s innovative privacy initiative was both strategic and technological, according to the Innovation Awards judges. It crossed multiple divisions of the organization and required extensive, planning, assessment and coordination of cross-sectional business units. Rather than collect customer consent on separate forms, ATB Financial designed a system to direct customers to a single point of entry and awareness. A privacy brochure enforced by a publicly available Customer Privacy Code was also created and distributed to all existing customers to capture one, uniform consent for portfolio management. This complex and intricate effort resulted in the one of the first online opt-outs made available for customers of financial institutions in Canada.

“As an Alberta-based financial institution, ATB Financial is very pleased to be recognized by the IAPP for its innovative privacy approach,” said Privacy Officer Sandra Smith-Frampton, CRM.

IAPP Privacy Innovation Technology Award
Voltage Security, Inc., won the technology award for its Voltage Identity-Based Encryption™ technology incorporated into its data protection solutions. Voltage IBE protects information on PCs (laptops, desktops, mobile and wireless devices) and in email communications, and enables compliance with a broad range of privacy guidelines and regulations, such as PCI, HIPAA, GLBA, PIPEDA and the Data Protection Act.

Voltage IBE solutions can be used to protect the privacy of information internally within an organization, such as HR and financial information; externally with business partners, brokers and the supply chain to protect company confidential information, such as pricing and other trade secrets; as well as with customers to protect personally identifiable information, such as credit card, Social Security and drivers license data. Voltage IBE solutions are in use by more than 250 world-leading organizations, and by partners such as Integro Insurance Brokers, Spheris, XL Global Services, Winterthur Life, Microsoft, NTT Communications, Symantec, Ciphertrust, Proofpoint and Tablus.
Marriott’s Chris Zoladz is Privacy Professional of the Year

The IAPP and Deloitte & Touche LLP (“Deloitte & Touche”) proudly presented Chris Zoladz, Vice President, Information Protection, Marriott International, with the IAPP/Deloitte & Touche Vanguard Award, which recognizes the privacy professional of 2006.

“Chris Zoladz is a pioneer of the nascent privacy profession,” said IAPP Board President Kirk M. Herath, CIPP/G, President of the IAPP Board of Directors and Chief Privacy Officer, Associate General Counsel, Nationwide Insurance Companies. “He was the first CPO for Marriott and he was one of the first leaders of the IAPP. As a mentor to many privacy professionals, I can think of no one more deserving for this year’s Vanguard Award.”

“Privacy is as much a key business issue as top-line growth, cost reduction, or tax optimization, and Deloitte & Touche is proud to recognize and support excellence in the privacy profession,” said Rena Mears, National Privacy & Data Protection leader in the Security & Privacy Services practice at Deloitte & Touche LLP, the co-sponsor of the Vanguard Award. “We support the Vanguard Award and remain deeply committed to advancing the privacy profession.”

Zoladz, a longtime committed privacy leader for the privacy industry and past president of the IAPP Board of Directors, was nominated in large part for his role as chairman of the Privacy Roundtable at Marriott, Hilton, Hyatt, Starwood and InterContinental. In this capacity, Zoladz spearheaded an initiative in this group to develop privacy training for hotel employees.

Zoladz, a Certified Information Privacy Professional, brought together this group of marketplace competitors to embrace the importance of launching a gold standard privacy training program for hotel employees. He not only had the vision, but also coordinated the logistics and arrangements with vendors for the program.

Lynn Goodendorf, Vice President of Data Privacy at InterContinental Hotel Group, praised Zoladz for his leadership.

“This effort led to a mandatory brand standard in our company that all hotel employees must be trained using this program,” said Goodendorf, who nominated Zoladz for the award.

“We have now deployed this training to over 2,500 hotels in the U.S., Canada and Mexico, in both English and Spanish. It takes a special kind of leadership to get fierce competitors to collaborate and Chris did it.”

IAPP Toronto Conference continued from page 11

Rogers added, “Customers create value for our companies in two ways: they pay us money today. They also create value for us in another way that is very hard to measure and many companies don’t bother.” Customers, she said, make decisions about whether they will do business with companies in the future.

Noting that companies often drive away a customer by strident applications of its policies, Rogers stressed that that approach deprives an organization of its most precious resource.

“When we take a customer’s point of view, it means treating different customers differently,” said Rogers.

“(Return On Customer) is also a philosophy of doing business based on earning a customer’s trust,” said Rogers, who added that privacy and data security are “the most tangible manifestations of trust.”

Rogers left an impression on many attendees, some of whom crowded around her after her presentation to ask her questions.

“Dr. Rogers was excellent — she stole the show,” remarked one privacy pro.

Added another, “Martha does an excellent job of engaging the audience.”

The Academy Comes to a Close But the Summit Beckons

The Academy came to a close after the Encore Sessions, programming that consistently has attracted the highest number of attendees and received the best ratings.

After leaving behind Toronto and our most successful Academy, the IAPP returned to York, Maine, where the staff already is deep into planning for our next event, the IAPP Privacy Summit, March 7-9, in Washington, D.C.

The momentum is building for our next conference, so don’t miss out on all that the IAPP consistently delivers to members and attendees. Stay tuned to the Daily Dashboard and our Web site, at www.privacyassociation.org, for registration and programming details.
Privacy Advisor Catches up with Author Don Tapscott


The Privacy Advisor (TPA): Can you explain how you became interested in the topic of privacy?

Tapscott: As a social activist in the 1960s, I became aware that the government kept a detailed file on me. I thought that was inappropriate because I was not a law-breaker.

TPA: In 1996, you and co-author, Dr. Ann Cavoukian, published, Who Knows: Safeguarding Your Privacy in a Networked World. What are some of the unexpected privacy issues you anticipated well before these concerns became evident in the marketplace?

Tapscott: In the early 1990s, I understood how the Net was going to revolutionize society and it occurred to me that non-government threats to privacy might eclipse “Big Brother.”

TPA: What are some of the predictions you made about privacy threats that did not come to fruition?

Tapscott: The book Who Knows stands up remarkably well. I can’t say that about everything I’ve written.

TPA: In your book, you described “digital crumbs” as pieces of information, that when taken together, add up to a whole individual profile. In your view, what are the inherent risks of this practice and should they be minimized, and if so, how?

“All the usual safeguards make sense. Don’t give away your birth date, Social Security number or other unnecessary information. Challenge vendors who want such.”

Tapscott: The solution is not to lay out or collect crumbs. The solution to safeguarding privacy is to have strict controls, voluntary and otherwise, regarding how those crumbs will be used.

TPA: It’s 2016. Given your track record for predictions about privacy threats, give us a few examples of the emerging privacy threats you see over the next decade.

Tapscott: With the recent actions of the U.S. and other governments, it turns out that “Big Brother” may in fact be less benign that I’ve implied in the past.

TPA: How do you recommend that people protect their personal privacy online?

Tapscott: All the usual safeguards make sense. Don’t give away your birth date, Social Security number or other unnecessary information. Challenge vendors who want such.

TPA: Can you tell us, generally, what topic your next book will tackle?

Tapscott: The book is called Wikinomics: How Mass Collaboration Changes Everything. Throughout history corporations have organized themselves according to strict hierarchical lines of authority. Everyone was a subordinate to someone else — employees versus managers, marketers versus customers, producers versus supply chain sub-contractors, companies versus the community. Today millions of media buffs now use blogs, wikis, chat rooms, and personal broadcasting to add their voices to a vociferous stream of dialogue and debate called the Blogosphere. Employees drive performance by collaborating with peers across organizational boundaries, creating what we call a wiki workplace. Customers become prosumers by getting engaged in co-creating goods and services rather than simply consuming the end product. So called “supply chains” work more effectively when the risk, reward and capability to complete major projects — including massively complex products like cars, motorcycles and airplanes — are distributed across planetary networks of partners. Mass collaboration is beginning to change many aspects of the economy.
Martha Rogers Joins Board of Directors of Click Tactics

Recognized as one of the world’s leading experts on customer-based business strategies and growing customer value, Peppers and Rogers Group founding partner Martha Rogers, Ph.D, has joined the Board of Click Tactics, Inc., a leading multichannel marketing services provider for Global 2000 companies.

Of this appointment, Click Tactics CEO, Andrew Frawley, said “Martha is one of the most influential business thought-leaders of our time, with an unwavering commitment to driving customer-centric concepts and practices forward. Her expertise and energy will give our customers a significant advantage in developing programs focused on moving their customer relationships and business growth to new levels.”

“Click Tactics is a company that is making enormous strides in winning the battle against the slow, impersonal and largely irrelevant marketing programs that have dominated the communications landscape for so long,” Dr. Rogers said. “Companies that have adopted the concept of one to one marketing will find the Click Tactics solution an efficient way to execute and evolve those principles in the market. I’m looking forward to working with this talented group to help their clients’ businesses grow.”

Business 2.0 magazine named Dr. Rogers one of the 19 most important business gurus of the past century. The World Technology Network recognized her as “an innovator most likely to create visionary ripple effects.” Accenture’s Institute for Strategic Change ranked her among the Global “Top 100 Business Intellectuals.”

With Don Peppers, Dr. Rogers has co-authored seven best-selling books, including: The One to One Future (Currency/Doubleday 1993), Enterprise One to One, One to One B2B and their newest book, Return on Customer (or ROC) released in June 2005. Their textbook, Managing Customer Relationships, has been adopted by dozens of universities around the world. The books have sold well over one million copies and appear in a total of 17 languages.

In August 2003, Peppers & Rogers Group joined Carlson Marketing Worldwide to provide clients with worldwide customer strategy, flawlessly executed, for bottom-line impact. As an Adjunct Professor at the Fuqua School of Business at Duke University, Dr. Rogers has helped to spearhead coursework at the MBA and Exec. Ed level on “Growing Your Business by Increasing the Value of the Customer Base.” She is also the co-director of the Duke Center for Customer Relationship Management. She is widely published in academic and trade journals, including, Harvard Business Review, Journal of Public Policy and Marketing, Journal of Advertising Research and Journal of Applied Psychology. She has been named International Sales and Marketing Executives’ Educator of the Year and with Don Peppers, she has been named Direct Marketer of the Year by DM Days New York.

Privacy Classifieds

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

SENIOR PROJECT MANAGER-PRIVACY
Wal-Mart Stores, Inc.
Bentonville, AR

CHIEF PRIVACY OFFICER
Roche Pharmaceuticals
Nutley, NJ

SENIOR PROJECT MANAGER – NATIONAL COMPLIANCE
Kaiser Permanente
Oakland, CA

PRIVACY CONSULTANTS
Samet Privacy, LLC
Los Angeles, CA

DIRECTOR–PRIVACY
Gap, Inc
San Francisco, CA

INFORMATION SECURITY ENGINEER
Lam Research
Fremont, CA

PRIVACY PROJECT COORDINATOR
Ernst & Young
New York, NY

PRIVACY SPECIALIST
Iron Mountain
Boston, MA

SENIOR ANALYST-COMPLIANCE
Prudential Financial
Newark, NJ
AOL Names Jules Polonetsky Chief Privacy Officer And Senior Vice President Consumer Advocacy

AOL recently announced the appointment of their first Chief Privacy Officer. Jules Polonetsky, CIPP, will lead all of AOL's activities related to privacy policies and procedures. He and his team will formulate and enforce standards for a wide range of consumer issues, including privacy, ad policy, accessibility, content guidelines, community practices, child safety and general online security. To support AOL's commitment to consumers and privacy, this team will also launch cross-corporate education and communications initiatives.

Polonetsky, a Board Member of the IAPP, joined AOL in 2002 from DoubleClick as their Chief Privacy Officer. He previously served as the New York City Consumer Affairs Commissioner for Mayor Rudolph Giuliani.

Shred-A-Thon Days Tackle ID Theft for Westchester Residents

Westchester County Executive Andrew J. Spano announced the launch of a mobile shredder machine to help residents combat identity theft. Allocated with recycling funds, the $60,000 shred-mobile has capacity to shred 150 pages at one time and hold up to one ton of shredded paper.

County spokeswoman Susan Tolchin said, “[the truck] is raising public awareness and physically doing something to help our residents prevent their identities from being stolen. We don’t want Westchester residents to have to go through the heartache, misery, aggravation and financial loss of having their identity stolen.”

This not-for-profit initiative is for residents only at household chemical clean-up day events held throughout the county and will not be offered to businesses. Residents’ personal papers will be shredded on-the-spot and recycled.

Left to right: Gary Brown, Westchester County Director of Consumer Protection; Andy Spano, Westchester County Executive and Anthony Landi, Westchester County Commissioner of Environmental Facilities.

Photos by Wasiayah Talib-Taylor of the Westchester County Executive’s Office

NASCIO Releases Research Brief for State CIOs

NASCIO’s Security and Privacy Committee has released its latest research brief, “Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?” This research examines how privacy in the state government context has evolved as a defining issue in response to rapidly changing technological advances and the complexities of a fast-paced world. It further explores some initial areas in which a state CIO may encounter privacy issues and offers potential ways of addressing those issues.

“Privacy is a particularly daunting challenge for state governments, because citizens have an expectation of openness and transparency. Yet, at the same time, states must foster citizens’ trust by ensuring that their private information remains that way,” said Brenda Decker, CIO, Nebraska, and NASCIO’s Security and Privacy Committee Co-Chair. “This brief starts us down the path of understanding how technology has changed the nature of privacy issues and how they can be effectively addressed.”

“We feel that the brief will be of assistance to state CIOs as they encounter privacy issues in many different contexts — from the implementation of new IT systems to the implementation of new laws with technology components. We then provide them with a wide-range of considerations for understanding how they can effectively manage and implement privacy protections and, ultimately, play a part in keeping the citizen trust,” said Mary Carroll, CIO, Ohio, and NASCIO Security and Privacy Committee Co-Chair.

This brief is available at www.nascio.org/publications/researchBrief.cfm
Facebook Adds More Privacy Controls

As Facebook relaxes its enrollment eligibility requirements to only a valid email address, members can now take advantage of the site’s industry-leading privacy controls.

Facebook’s latest expansion makes it possible for anyone with a valid email address to join Facebook and interact with their friends and people in their region. New users are still required to prove affiliation to access an existing college or work network, and are also asked to validate their mobile phone number to verify their account.

Consistent with Facebook’s unique network structure, people’s profiles are only accessible to other people in the same network and to confirmed friends. With this expansion, Facebook has launched additional privacy controls that allow every user to: block other users in specific networks from searching for his or her name, prevent people in those networks from messaging, poking and adding him or her as a friend, and control whether his or her profile picture shows up in search results.

“We are expanding to respond to the requests of millions of people who want to be part of Facebook, but haven’t been able to until (now)’’ said Mark Zuckerberg, founder and CEO of Facebook. “About one-third of Facebook’s college users have already graduated and are now interacting with more people outside of their schools and work environment.”

(See Calendar to register for Facebook audio conference on December 7, 2006)

ChoicePoint Names Carol DiBattiste General Counsel and Chief Privacy Officer

Carol DiBattiste, former federal prosecutor and executive with the U.S. Department of Justice, has been named ChoicePoint’s General Counsel and Chief Privacy Officer, after having served as the company’s Chief Credentialing, Compliance and Privacy Officer since April 2005.

“Carol’s knowledge and experience make her well suited to addressing the broader opportunities ahead of us,” said ChoicePoint Chairman and CEO, Derek Smith.

Announcing Extension of Public Comment Period Related to Prerecorded Telemarketing

The FTC has approved the publication of a Federal Register notice announcing the extension of the public comment period on two proposed amendments to the Telemarketing Sales Rule (TSR). The two proposals were announced in a previous Federal Register notice on October 4, 2006. One proposal would explicitly prohibit using prerecorded messages in telemarketing calls answered by a consumer (unless the consumer has given prior written consent to receive such prerecorded message calls). The other proposal would change the method of calculating the maximum allowable rate of call abandonment from a “per day per calling campaign” standard to a “per thirty days per calling campaign” standard. The public comment period will now expire on December 18, 2006.

Chief Privacy Officer Still a “Hot Job” Today

The privacy profession has seen a surge in its ranks as companies focus on proactive ways to prevent data breaches and improve data security, according to attorney Joe Murphy who specializes in ethics and compliance, recently interviewed for the Courier Post Online.

The article describes a CPO’s daily duties and recommendations if your business is too small to afford a CPO and provides some additional privacy resources, among them a visit to the IAPP’s Web site.
privacy guidelines. The user is presented with a link to the privacy statement as well as a number of privacy-related options that govern how their data is collected and used, including whether data about their music library is sent to Microsoft in order to display additional information (such as album art), whether licenses for protected content are acquired automatically, or whether the player remembers the user’s viewing and listening history. The user also is asked whether he or she wishes to send data about player usage and errors to Microsoft as part of the company’s Customer Experience Improvement Program.

With the release of the public Privacy Guidelines for Developing Software Products and Services, Microsoft hopes to promote a broader industry discussion about development guidelines to help protect individual privacy and ensure appropriate data governance. The benefits of such guidelines are clear; not only do consistent user experiences and development practices help protect against misuse of data and other privacy violations, they also promote trust among customers and organizations. Additionally, a reputation for responsible privacy protection has become a market differentiator for companies, attracting and retaining customers based on clear standards and reliable experiences.

No single company has all the answers when it comes to privacy. Addressing these issues requires broad collaboration among software developers, governments and industry organizations. In releasing these guidelines, our hope is that we can further the discussion on how consistent software development practices can make a difference in protecting privacy and preserving public trust in computing.

As Microsoft’s Chief Privacy Strategist, Peter Cullen, CIPP, is directly responsible for managing the development and implementation of programs that enhance the privacy of Microsoft products, services, processes and systems, both internally and worldwide. With more than a decade of privacy and data protection policy expertise, he serves as a leading advocate for strong and innovative personal information privacy and data safeguards, meeting regularly with global industry and public policy leaders and frequently speaking at international conferences. Cullen is a member of the IAPP Board of Directors.