



Employee monitoring technologies and data privacy— no one-size-fits-all globally

By Lothar Determann and Lars Brauer

When it comes to protecting intellectual property, ensuring productivity, and identifying bad behavior, the tools available to employers are many and powerful. But their use poses legal risks and challenges. In this article, Lothar Determann and Lars Brauer shed light on the legal environment surrounding employee monitoring.

This is the first article in a Privacy Advisor series on workplace and employee privacy. In future months we'll explore the privacy-related concerns surrounding background checks, employee surveillance, safekeeping HR data, and more.

State-of-the-art network security tools offer the capability to monitor a variety of aspects of an individual's computer use. Such tools not only save the addresses of Web sites visited or the e-mail addresses of senders and recipients, but also they permit the review of the actual content of data sent and received, i.e., the actual look of the Web sites visited the way the user saw them, form data submitted by the user to those Web sites, and the full text of e-mails and chat sessions between the user and third parties. Employers of all sizes are, increasingly, using these tools to monitor employees' IT use. As these tools gain



Lothar Determann



Lars Brauer

in popularity, companies—particularly multinationals—should be aware of the legal restrictions that apply to their deployment in many jurisdictions.

See, Employee monitoring, page 3

Enterprise data management: the privacy professional's role in this emerging trend

Enterprise data management is about breaking down the silos that can constrain the success of an organization's overall data governance efforts. Maria Villar explains the role of the privacy professional in the emerging trend toward EDM.

By Maria Villar

The enterprise data management program

The effective management of sensitive customer and employee data is at the heart of an effective privacy program. Programs that identify, store, process, and safeguard this data, in compliance with company and government privacy requirements, becomes the responsibility of the chief privacy officer, working in partnership with the company's business and IT functions. Typically, the data management programs to comply with the company's privacy policies are separate and unique from the company's other data management programs that manage the data requirements for Sarbanes-Oxley compliance, risk management, customer relationship management, and human resource management. However, a new data man-



Maria Villar

See, Enterprise Data Management, page 8

This Month

Notes from the Executive Directorpage	2
Global Privacy Dispatches	page 10
Facebook: The future of service of process?	page 15
KnowledgeNet Recap	page 16
What are you reading?	page 17
Calendar of Events	page 18
Certification Graduates	page 19
Privacy Classifieds	page 19
Privacy News	page 22

THE PRIVACY ADVISOR

Editor

Kirk J. Nahra, CIPP, Wiley Rein LLP
knahra@wileyrein.com
+202.719.7335

Publications Director

Tracey Bentley
tracey@privacyassociation.org
+207.351.1500

The Privacy Advisor (ISSN: 1532-1509) is published monthly by the International Association of Privacy Professionals and distributed only to IAPP members.

ADVISORY BOARD

Nathan Brooks, CIPP, General Counsel,
U.S. ISS Agency, LLC

Keith P. Enright, CIPP, CIPP/G, VP, Privacy & Chief Privacy Officer, Macy's Inc.

Debra Farber, CIPP, CIPP/G, Managing Consultant,
IBM Corporation

Jill Frisby, CIPP, Manager, Crowe Horwath, LLP

Brian Hengesbaugh, CIPP, Partner, Privacy/Information Technology/E-Commerce, Baker & McKenzie LLP

Steven B. Heymann, CIPP, VP, Compliance and Information Practices, Experian

Jim Keese, CIPP, Global Privacy Officer, VP Records & Information Mgmt., The Western Union Company

Robert Mahini, Attorney, Federal Trade Commission

Fleming Moos, Lawyer, DLA Piper UK LLP

David Morgan, Director, Privacy Research,
Camouflage Software, Inc.

Lydia E. Payne-Johnson, CIPP, Financial Services Privacy Consultant, PricewaterhouseCoopers, LLP

Dan Ruch, Privacy and Data Protection Specialist

Luis Salazar, CIPP, Shareholder, Greenberg Traurig

Julie Sinar, CIPP, Information Management Consultant, PricewaterhouseCoopers, LLP

Kathleen Street, CIPP, Asst. Vice President, Corporate Compliance and Privacy, Children's Health System

Frances Wiet, CIPP, Chief Privacy Officer, Hewitt Associates LLC

To Join the IAPP, call:

+800.266.6501

Advertising and Sales, call:

+800.266.6501

Postmaster

Send address changes to:

IAPP
170 Cider Hill Road
York, Maine 03909

Subscription Price

The Privacy Advisor is a benefit of membership to the IAPP. Nonmember subscriptions are available at \$199 per year.

Requests to Reprint

Tracey Bentley
tracey@privacyassociation.org

Copyright 2009 by the International Association of Privacy Professionals. All rights reserved. Facsimile reproduction, including photocopy or xerographic reproduction, is strictly prohibited under copyright laws.

Notes From the Executive Director

Beyond compliance

With all of the good work accomplished in the data privacy field each day, it is easy to sometimes forget how far there is to go. A funny thing happened recently to remind me that, despite all the progress of this profession, our work is not done.

Like many organizations, the IAPP monitors the Web for use of its name. Earlier this month our name popped up in the privacy policy of a national nonprofit organization with whom the IAPP has never been affiliated. A brief inspection of the policy revealed its origins—the policy of an organization with which the IAPP has been affiliated.

A closer look revealed that this organization had copied wholesale the privacy policy of an unrelated entity and, presumably, used the find-replace function to insert its name where the original organization's name had been—product names, affiliations, and industry-specific citations remained.

The effort in the marketplace to drop policies onto every Web site has been successful. But we cannot disconnect the posting of a policy from the active management of a privacy program. This copy-and-paste policy approach, while quick, undercuts the valuable and intellectually strenuous work of developing sound, thoughtful privacy policies that help establish trust in the marketplace.

In a speech earlier this month, EU Consumer Protection Commissioner Meglena Kuneva cited the need for a heightened level of Internet trust and privacy awareness to help Europeans feel comfortable engaging in e-commerce. She said: "Confidence and trust is the new currency in Europe." Her words could not be more timely.

Ours is not a cookie-cutter profession. The convoluted nature of and tempestuous legal environment surrounding data privacy requires hands-on, highly tailored solutions. Each day technological advances drive new innovations in goods and services that require more thought, more effort on the part of those of us dedicated to privacy work. There's a heck of a lot more to that than a click-and-drop privacy policy.

I hope the aforementioned organization enlists the expertise of a privacy professional soon. And I hope to see many of you next month at the IAPP Practical Privacy Series in Silicon Valley, where Heartland Payment Systems Chairman and CEO Bob Carr will discuss his company's data breach, and what Heartland is doing to help others prevent data breaches.



J. Trevor Hughes, CIPP
Executive Director, IAPP

Employee monitoring

continued from page 1

Providers of network security solutions do not make a secret out of the intrusiveness of their products. One manufacturer of network security tools describes its product as offering “continuous and complete real time surveillance” and “superior drill down forensic analysis, down to packet level” as the product’s key benefits. Another manufacturer advertises its offering as a system that “protects against inadvertent or intentional data leakage by allowing companies to proactively protect sensitive information from leaving the network and enforce correct business processes.”

Many businesses find these monitoring technologies helpful in detecting and preventing the theft of company intellectual property, excessive personal computer use, and illegal or inappropriate employee behavior; or in responding to discovery requests. Companies may also use these technologies to comply with statutory, regulatory, or industry requirements. Examples include obligations relating to the treatment of accounting or audit-related complaints under the Sarbanes-Oxley Act, mandates for the prevention of harassment in the workplace under Title VII of the Civil Rights Act, and stock exchange rules requiring retention of correspondence with the public.

At the same time, the use of these technologies poses a number of legal risks and challenges. Under both domestic and international laws, using monitoring tools to their fullest extent can be illegal or, at a minimum, require affirmative steps to become legal. In

“Interception means acquiring the contents of such communication during transmission...”

the United States, using monitoring tools may violate traditional wiretapping laws that were originally enacted to prohibit third parties from listening in on private phone conversations, but which are broad enough to cover interception of e-mail, instant messaging, and web traffic. Internationally, employee monitoring will often run afoul of the broad omnibus data protection laws in effect in many countries, including the entire European Community (EC), unless such monitoring is made subject to strict limitations.

Restrictions on monitoring of Web and e-mail traffic

The federal Electronic Communications Privacy Act (ECPA) prohibits the “interception of electronic communications.” Most of the activities an employee engages in while connected to a network (e.g., web traffic, e-mail and instant messenger sessions) qualify as electronic communications for these purposes. Interception means acquiring the contents of such communication during transmission, and “contents,” in turn, is defined to include “any information concerning the substance, purport, or meaning of that communication.” This means that the ECPA does not prohibit the mere collection of information about the activities engaged in by an employee online (e.g., the time spent online or the volume of data transferred). Rather, it protects the secrecy of the actual data transmitted to and from an employee’s workstation (e.g., the actual appearance of Web sites visited, form data submitted, subject lines and bodies of e-mails sent and received and transcripts of chat sessions, etc...).

There is generally no liability for interception under the ECPA as long as “one of the parties to the communication has given prior consent to such interception....” Thus, with valid consent from the employees involved, the recording of web traffic data, e-mails, and IM sessions will generally not violate the ECPA, even if the communica-

See, Employee monitoring, page 4

iapp

international association of privacy professionals

170 Cider Hill Road
York, ME 03909
Phone: +800.266.6501 or +207.351.1500
Fax: +207.351.1501
Email: information@privacyassociation.org

The Privacy Advisor is the official monthly newsletter of the International Association of Privacy Professionals. All active association members automatically receive a subscription to *The Privacy Advisor* as a membership benefit. For details about joining IAPP, please use the above contact information.

BOARD OF DIRECTORS

President

Jonathan D. Avila, CIPP, Vice President – Counsel, Chief Privacy Officer, The Walt Disney Company, Burbank, CA

Vice President

Nuala O’Connor Kelly, CIPP/G, Chief Privacy Leader, General Electric Company, Washington, DC

Treasurer

David Hoffman, CIPP, Director of Security Policy and Global Privacy Officer, Intel Corp., Germany

Secretary

Amy Yates, CIPP, Director, Privacy and Data Protection, Deloitte & Touche LLP, Chicago, IL

Past President

Sandra R. Hughes, CIPP, Global Ethics, Compliance and Privacy Executive, The Procter & Gamble Company, Cincinnati, OH

Executive Director, IAPP

J. Trevor Hughes, CIPP, York, ME

Bojana Bellamy, Director of Data Privacy, Accenture, London

Agnes Bundy Scanlan, Esq., CIPP, Counsel, Goodwin Procter LLP, Boston, MA

Malcolm Crompton, Managing Director, Information Integrity Solutions Pty Ltd., Chippendale, Australia

Stan Crosley, Esq., CIPP, Chief Privacy Officer, Eli Lilly and Co., Indianapolis, IN

Dean Forbes, CIPP, Senior Director Global Privacy, Schering-Plough Corp., Kenilworth, NJ

D. Reed Freeman, Jr., CIPP, Partner, Kelley Drye & Warren, LLP, Washington, DC

Jeff Green, CIPP/C, VP, Global Compliance & Chief Privacy Officer, RBC, Toronto, ON

Kirk M. Herath, CIPP/G, Associate Vice President, Chief Privacy Officer, Associate General Counsel, Nationwide Insurance Companies, Columbus, OH

Jane Horvath, Senior Privacy Counsel, Google

Alexander W. Joel, CIPP/G, Civil Liberties Protection Officer, Office of the Director of National Intelligence, Bethesda, MD

Harriet Pearson, CIPP, Vice President, Regulatory Policy and Chief Privacy Officer, IBM Corporation, Armonk, NY

Zoe Strickland, CIPP/G, Vice President, Chief Privacy Officer, Wal-Mart Stores, Inc.

Brian Tretick, CIPP, Executive Director, Ernst & Young, McLean, VA

Ex Officio Board Member

Kirk J. Nahra, CIPP, Partner, Wiley Rein LLP, Washington, DC



Employee monitoring*continued from page 3*

tion is with an outside party unaware of the recording. Some states expressly require notice to employees before monitoring mechanisms can be deployed in the workplace. For companies with employees located in one of those states, it will generally make sense to combine this mandatory notice with the request for consent.

The ECPA is reflected in the actual practices of most companies today. These companies take advantage of the consent defense by including information about their monitoring activities in their employee handbooks, separate IT-use policies, or on screen banners that appear upon every system logon, and by requiring employees to acknowledge this information by way of a signature or mouse click. Under U.S. federal law, these kinds of measures should generally be sufficient to avoid liability for monitoring an employee's activities. While most HR and IT professionals have at least a vague idea that the situation may not be as easy in other countries, many do not know that their company's monitoring activities may be a cause for concern, even domestically. That is true, for instance, if the company, the employees in question, or both, are located in California or certain other states.

All-party consent requirements

California's anti-wiretapping statute is similar to the ECPA in that it prohibits anyone from attempting to read or learn the contents or meaning of electronic communications. However, while the consent of one party suffices as a defense under the federal statute, interception is illegal under the California provision unless all parties to the communication have consented. Other states, including Florida and Illinois, have similar all-party consent statutes in place.

In all party consent states, relying on employee consent alone to justify the recording of web, e-mail, and IM traffic will not completely shield an

"But it is more difficult to inform third-party Web sites or e-mail and text message recipients of monitoring practices, let alone ask for upfront consent..."

employer from liability. An employer will generally be able to justify the monitoring of purely intra-company communications in this manner, given that all parties involved will be the employer's own employees or independent contractors who have acknowledged in writing or electronically that their activities may be monitored. Accordingly, cases dealing with monitoring of employee communications have generally been decided in favor of the employer, even in all-party consent states.

Employee consent alone, however, does not preclude liability for communications with outside parties. Employers might face civil or even criminal liability if such third parties were to complain or sue. Situations in which third parties are likely to find out that their communications were recorded arise, for instance, when the employer wants or has to use the findings of monitoring initiatives to bring suits against the employee or the third party, or to respond to government investigations. In a time of growing awareness of data privacy issues among the general public, and at the same time heightened investigative activity, it seems likely that the privacy law dimension of private party monitoring activities will become a more prevalent theme of suits, complaints, and defenses.

Companies can avoid liability by obtaining consent from all parties to a communication. Call center operators, for example, commonly state at the beginning of a call that the call is monitored. Some operators specifically ask whether the caller agrees with monitoring; others rely on implied consent by

callers who continue with the call after receiving the notice regarding monitoring. Similar notices could be displayed in instant messenger and web chat communications.

But it is more difficult to inform third-party Web sites or e-mail and text message recipients of monitoring practices, let alone ask for upfront consent (as the first message presumably is subject to the monitoring).

Theoretically, a company could, as a matter of policy, try to broadcast its monitoring practices to all customers, suppliers, service providers, and other business partners, perhaps even friends and family members of employees who may engage in electronic communication with company employees. In such notices, the company could inform recipients that their communications are subject to monitoring and recording. With respect to suppliers, companies may be able to impose duties on the suppliers to obtain express consent from the individuals. With respect to customers, many companies may shun away from asking for upfront express consent in the early phases of a relationship, but in quite a few instances, companies may be able to rely on implied consent after posting transparent statements about monitoring policies on their Web sites. Also, with respect to monitoring employee access to third-party Web sites and e-mail correspondence, companies can take additional steps and assert additional arguments to establish implied consent by the outside party:

Implied consent: Web sites

"Interception" for purposes of the wiretapping provisions of the ECPA and other wiretapping laws requires acquisition of content during transmission. Therefore, an employer who merely finds out what Web sites an employee viewed and then visits those Web sites after the fact as they then appear does not "intercept." However, the modern network monitoring tools we are analyzing here record the communication between the user and the Web site (including the request to load each page

of the site, the transmission of data by the site to the employer's computer, and any submission of form data by the employee to the site) as it passes through the network. Under those circumstances, the ECPA and similar wiretapping laws generally apply and employers may therefore not use such tools to monitor their employees' web communications without consent or another justification.

In the case of publicly accessible Web sites with which employees are communicating on the job, the Web site operator—the other party to such communications whose consent would be required—should be aware that monitoring practices are commonplace in many companies. A Web site operator will generally be unlikely to have objections to employers being able to view its site after it has been visited by an employee, particularly when any member of the public can view the site anyway. Yet, even many publicly accessible Web sites thrive or benefit from access by employees during work hours. Thus, the Web site operators have an interest in employers not monitoring employee access to their Web sites.

Implied consent: e-mails

Monitoring of employee e-mails presents additional issues. As with Web site communications, wiretapping laws typically encompass technological tools that monitor or record the content of e-mails as they are transmitted through the network. And again, even assuming employees have validly consented to having their use of both company and personal e-mail use on work computers monitored, consent has to be on all sides. Therefore, senders and recipients of e-mails received or sent by employees must also have consented to the employer's monitoring activities for the employer to escape liability.

Implied consent can arguably be assumed where outside parties contact employees at their work e-mail address or via a dialog box on a company web page. One might argue that in doing so, these individuals should expect to

be communicating with the company as an organization, rather than with the particular individual they are contacting, and should therefore have no expectation of privacy as to how their communication is passed on within the company. However, such an argument is vulnerable to attack based on the fact that wiretapping statutes typically do not require that the intercepted communication be confidential in nature. Thus, a lowered (or even a missing) expectation of privacy in the communication alone does not serve as a substitute for the required consent. Accordingly, although it could be argued that a lowered expectation of privacy also applies to individuals calling a company's call center, implied consent is not generally assumed with respect to such callers without an announcement that calls are monitored.

Employers can reduce the expectation of privacy by outsiders by placing a notice at the bottom of all outbound e-mails sent from corporate e-mail accounts. In doing so, the employer gains an argument that, at least when the third-party contacts its employee again after receiving an e-mail with this disclaimer, the third party is on notice of, and impliedly consents to, the employer's monitoring activities. Similar notices could be included on the compa-

ny Web site and made accessible from any page on which visitors can submit information to the company.

In scenarios other than the one where third parties contact a company employee at his or her work e-mail address, establishing consent on the part of the third party will be more difficult. For example, monitoring tools configured to record all information transmitted via a company network will generally also capture personal e-mails sent or received by an employee at his or her personal e-mail address, if read via web-mail from a work computer. Friends, family members, and other third parties who send or receive such e-mails will often be unaware that the employer has access to these e-mails. Therefore, employers will find it difficult to argue that these parties have consented to being monitored. Employers can attempt to reduce their risk of exposure somewhat by requiring employees to notify their regular e-mail contacts that even e-mails sent to their personal accounts are subject to monitoring if read at work. It seems unlikely that all employees would actually adhere to such a policy, but from a purely legal perspective, employers could benefit from implementing strict outbound e-

See, Employee monitoring, page 6



Employee monitoring*continued from page 5*

mail notice requirements, because such notices will help reduce expectations of privacy. Also, the mere existence of a notice requirement on the employee may help employers dissuade employees and third parties, whose loyalties are with employees in particular disputes, from raising the privacy concern in such disputes (because it was arguably the employee's fault that the third party did not know about the monitoring). Of course, companies also need to carefully consider the impact that such notices will have on their employee and customer relationships and consider whether less actual monitoring is the better option overall (monitoring with less notice, on the other hand, is typically not an acceptable option, as we discuss in this article).

Global perspective

In a global context, legal issues relating to employee monitoring arise not only under laws that resemble wire-tapping statutes in the United States, but also under omnibus data protection laws in place all across Europe and in other parts of the world. For instance, national laws passed by the various EU member states broadly prohibit a host of actions with respect to personal data (i.e., data relating to an identified or identifiable individual) absent consent or another means of justification. The prohibited actions include collection, processing, recording, storage, retrieval, and disclosure by transmission, all of which are essential parts of the functionality of many modern-day network security tools.

While required to implement the level of personal data protection provided for in the EU Data Privacy Directive, the legislatures of EU member states are free to impose additional mandates, as are the administrative agencies in charge of enforcement. Many have done so. For instance, in Germany and Italy, only individualized, written consent will justify any level of employee monitoring



and merely displaying an information banner upon login and then relying on implied consent would not be acceptable. Even if an employer has observed all formal requirements in obtaining consent, the validity of such consent may still be challenged (and has been challenged successfully) on the ground that in the employer-employee relationship, it cannot be considered freely given. One way to address this problem would be to give employees in problematic countries the ability to temporarily switch off all monitoring tools, e.g., in order to engage in personal communications without being recorded. Excessive use of this capability could be addressed on a case-by-case basis.

An employer who has managed to obtain valid consent from all of its employees may still be far from compliant with local data protection laws. A number of EU member states—including Germany, Italy, the Netherlands, Spain, and the United Kingdom—strictly prohibit ongoing monitoring of employee communications and permit electronic monitoring only in very limited circumstances (e.g., where an employer already has concrete suspicions of wrongdoing against particular employees) and subject to significant restrictions with respect to the duration, mode, and subjects of the monitoring activities. Several jurisdictions world-

wide—including France, the Netherlands, and Israel—require filings with data protection or labor authorities, while others—France, Germany, Italy, the Netherlands, and China—require employers to consult or at least notify trade unions or other employee representative bodies before subjecting their employees to surveillance measures.

Lessons for multinational employers

Because many multinational companies have centralized IT systems that process data flows from office locations in multiple countries, deploying network monitoring tools in one country can have implications under the laws of a number of jurisdictions at once. Choosing a state or country with no or few legal restrictions on employee monitoring as the physical location of their IT systems will not shield such companies from exposure in jurisdictions with more stringent requirements. Regardless of where the equipment in question is located, a complaint by an employee in a country with a high level of data protection can trigger investigations and suits by data protection authorities, trade unions, consumer watchdogs, and similar organizations, and can also lead to criminal complaints. Employers found in non-compliance may face steep penalties, damages awards, and possibly even prison

time, along with plenty of bad press, as some recent examples show.

Recently, the CEO of Deutsche Bahn AG resigned for questionable data processing practices that included automated comparisons of the addresses and bank account information of 175,000 employees with those of Deutsche Bahn suppliers, performed in an effort to uncover instances of fraud, nepotism, and bribery. Prosecutors are currently considering whether further investigations against the management of Deutsche Bahn are warranted. In September 2008, German authorities ordered discount retailer Lidl to pay fines totaling around 1.5 million Euros for a variety of alleged data protection violations against its employees, including monitoring employees and customers through the use of in-store hidden cameras to counter a theft wave. Earlier last year, Deutsche Telekom was the center of attention when the company admitted to having collected and

reviewed telephone call data of its directors and executives in order to investigate management irregularities.

Deutsche Telekom reacted by creating a management board position dedicated to data privacy and security matters. The fact that even companies based in Europe, with its long-time emphasis on data protection, struggle with privacy compliance shows that it is imperative for U.S. companies with operations

abroad to obtain legal advice on the implications of their contemplated monitoring activities under the laws of all jurisdictions in which affected employees are located.

Most multinational companies cannot refrain from the use of monitoring technology altogether. They need to engage in some monitoring to satisfy their legal obligations to protect assets and company data (including trade secrets and personal data), provide a harassment-free workplace, and ensure compliance with statutory, regulatory, or industry requirements. But, multinational companies should consider that some of the applicable requirements may only be applicable in particular countries (such as the United States), where the relevant technologies also raise privacy concerns to a lesser degree. In other countries, the privacy concerns weigh heavier, and companies are not required

"In other countries, the privacy concerns weigh heavier, and companies are not required or expected to engage in monitoring to the same extent."

See, Employee monitoring, page 20

Stay on Top of the Latest Legislative Action with

Privacy Tracker

Timely, easy-to-read recaps of the state and federal privacy bills you need to watch.

When you subscribe to *Privacy Tracker*, you get access to:

- Weekly e-mail updates of the week's legislative action on privacy bills, and highlights of multi-state trends and hot bills that are quickly gaining traction
- Print newsletters featuring articles written by an expert in a different practice area each month and a recap of the month's legislation
- Monthly calls with leading privacy experts on the latest issues
- The *Privacy Tracker* Web site, which includes archives of all past newsletters, calls and updates

Subscribe Now

www.privacytracker.org

Annual subscriptions are just \$475.

Enterprise data management

continued from page 1

agement trend is emerging. Leading companies are consolidating these silo data management programs into one Enterprise Data Management (EDM) program and appointing a chief data officer.

Consolidating silo data management programs has many benefits but comes with implementation challenges.

Benefits include increased efficiency and cost savings by using common technologies, processes, and organizational structures. Just as important is the coordination of activities on the same data. Customer and employee data are important to the company's marketing, sales, financial, customer service, and supply chain processes. Coordinating how sensitive data is created, stored, and safeguarded for the good of all the data users ensures that one division's requirements don't override the needs of another. Additionally, a company-wide EDM program focuses senior executive attention to business data. Business data is handled as a "company asset," similar to other assets like products, people, and capital.

With significant benefits, come implementation challenges. An EDM program requires cross-division and cross-process coordination. As in any other cross-company program, an effective leader must be chosen—one who can bring various, conflicting requirements together—and governance must be established to prioritize the data activities across the company. The appropriate funding and metrics must be established to ensure the company's return on investment. While all groups participate, at times the needs of the enterprise may override the needs of the few. Strong senior executive support is essential. The chief privacy officer, as well as other key business leaders—the chief finance officer, the chief risk officer and chief information officer—will all need to actively participate to ensure their data requirements are addressed.

Leading companies in industries such as technology, finance, and B2B are implementing EDM programs. For

privacy professionals, the new emerging data management program should be incorporated into the privacy program and leveraged in the following ways:

- 1) Use the corporate EDM resources in the privacy program.
- 2) Participate in the data governance program.
- 3) Partner with the EDM leaders (chief data officer) to champion business data as a company asset. Lead by example in the privacy organization.

Use the corporate EDM resources in a privacy program

An enterprise data management program offers corporate resources that can be used to implement an effective privacy program:

Enterprise Metadata Repository: the enterprise metadata repository is a corporate database that contains important business and technical information about the company's data. The repository is maintained by the IT organization but owned by the EDM leader. For the privacy program, the enterprise metadata repository would be used to log all the databases where sensitive data is stored. The privacy organization can also request other important information, such as the business and technical owner and users of the database, to be

logged in the repository in support of the privacy requirements.

Critical Data Element Identification:

An EDM program typically starts by identifying the most critical business data to manage. The information is gathered by surveying key stakeholders from across the company. The stakeholders identify the data elements that most materially affect the results of the company's financial, regulatory, and business processes and reporting. Sensitive data fits within the regulatory criteria and therefore is added to the critical data element list. The critical data element identification step also identifies the various business processes that depend on the same data. This is valuable information for the privacy program. The EDM program ensures information about the critical data element is kept in the enterprise metadata repository, and controls for adding, updating, and deleting the critical data list are in place.

Business Data Stewards: Business data stewards are new roles in the enterprise data management program. Stewards are business leaders within the business functions who are responsible for driving the implementation of the enterprise data management program. They "steward" the data created in their business process to ensure that it meets all company needs. The business data stewards for customer and



employee data, which typically resides in the sales and human resource functions, should be leveraged in the privacy program. The business data stewards partner with privacy professionals to ensure the privacy requirements are implemented in their data.

Data Profiling Tools: New tools exist that allow databases to be searched and better understood. In the privacy program, often times the location of all the stored NPI data across the company is not known. Data profiling tools can be used to investigate databases for sensitive data. Technical skills are required to run the tools, therefore the IT organization will also need to be involved.

Processes/Training for Creating, Updating, and Deleting Data: An Enterprise Data Management program will review the existing processes for creating, updating, and deleting (CRUD) the critical data. These processes will be enhanced to ensure data requirements and quality controls are in place. Training will be enhanced to ensure employees understand the new procedures. The privacy programs should leverage the new CRUD processes and training to incorporate privacy policy controls.

Privacy professional's role in the enterprise data governance program

A governance program is necessary to coordinate and manage the various cross-division and cross-process data requirements. The data governance forum(s) is chaired by the EDM lead, the chief data officer, or another appointed executive in the company. The chief marketing officer or chief finance officer may play this role because these leaders understand the need for high-quality, well-managed data. Executive representatives from across the business, operations, technology, compliance, and finance functions participate. The chief privacy officer, or his or her representative, ensures the privacy requirements are communicated, understood, and prioritized. Specifically, the privacy organization will participate in the following governance activities:



Critical data identification process: The privacy organization identifies the sensitive data elements in the critical data element identification process and the appropriate business and technical information to be collected and stored.

Identifying legal requirements: The privacy professional communicates all privacy state, federal, and country privacy legal requirements to be implemented in the data controls and training.

Data initiative prioritization: The chief privacy officer participates in the executive decision-making process to prioritize and fund corporate data initiatives and ensure the initiatives comply with privacy program requirements and implementation timelines.

Data performance metrics: The chief privacy officer participates in setting the performance metrics on key data initiatives and participates in the periodic reviews of performance metrics.

Data archiving, standards, and controls: The privacy organization reviews and approves the corporate processes for data archiving and data controls to ensure compliance with the privacy requirements. The privacy organization would also incorporate privacy requirements for collecting, updating, and deleting sensitive information in new data standards developed as part of the EDM program.

The chief privacy officer and the chief data officer

Both the chief privacy officer and the chief data officer (CDO) share a common goal: safeguarding and stewarding the company's critical data. While the CDO's data scope includes all the critical com-

pany data, the chief privacy officer's role is growing to include more data.

In companies where an enterprise data management program is not yet in place, the privacy organization may be the first to implement data management capabilities such as data standards, data tools, and data processes for managing sensitive data. These capabilities then can be re-used to manage other company data once an EDM program is implemented. In fact, the chief privacy officer can sell the need for an enterprise data management program to other C executives in the company because of his or her unique perspective into the growing need to manage an ever-increasing set of data.

The chief privacy officer's involvement provides much-needed executive sponsorship for the overall data program, and he or she can influence business peers to participate actively in the program. The privacy organization can also lead by example in implementing the EDM standards within their team. The privacy organization can also re-enforce the enterprise data management program and standards in the privacy specific training and controls.

The emerging enterprise data management trend provides the privacy professional and the chief privacy officer an opportunity to champion data as a "business asset" and simultaneously increase the effectiveness of their privacy programs. As the role continues to evolve, the chief privacy officer may even be in the best position to be the chief data officer.

Maria Villar is a recognized expert in enterprise data management and data governance with more than 25 years professional experience. She has held senior executive positions in the technology and financial sectors, where she was responsible for data quality, governance, architecture, and database technology solutions. She is the co-author of the book: Managing Your Business Data: From Chaos to Confidence. She can be reached at mariavillar@yahoo.com.

Global Privacy Dispatches

CANADA

By Terry McQuay, CIPP, CIPP/C

Virtual worlds research report

The Office of the Privacy Commissioner of Canada (OPC) recently released the results of research it commissioned to examine the privacy implications of virtual worlds such as Second Life. The concluding report consists of four parts:



Terry McQuay

Part I describes Linden Lab, Second Life and activities that Second Life residents pursue in-world.

Part II discusses the privacy of Canadians who register with Second Life, examining Linden Lab's Terms of Service and Privacy Policy.

Part III examines how residents can protect their privacy in-world, how easily avatars can be traced to the identity of the person controlling the avatar and the potential for in-world surveillance.

Part IV touches on business data practices within Second Life.

What is Second Life?

Second Life is an online community where users, via their avatars, interact with other 'residents' and engage in real-world activities such as purchasing land, constructing buildings, and creating objects and actions for their avatars.

Although residents interact in an online, imaginary environment, Second Life retains economic and legal connections to the real world. For example, the site recognizes residents' intellectual property rights and allows them to

generate real-world income. Just like in the real world, Second Life encompasses some of a community's less desirable attributes, such as virtual prostitution and drug use. Residents have also introduced adult content onto Second Life, prompting the creation of a Teen Second Life for those under the age of 18. Adults are prohibited from Teen Second Life and minors are not allowed on Second Life.

Real-world institutions on Second Life

The research report notes that real-world institutions such as government organizations, businesses, educational institutions, and nonprofit organizations have also established presences on Second Life. A number of Canadian organizations are among those who use Second Life to promote their real-world brands, products, services, and activities. The Université Laval has a Second Life campus where the school's communications faculty offers tours to Second Life residents; the president and CEO of the Northern Alberta Institute of Technology uses Second Life for meetings, instruction, and student recruitment; and law firm Davis LLP opened a Second Life office for building rapport and credibility with video-game business clientele.

Second Life and Canadian law

Linden Lab's Terms of Service state that resident data is subject only to U.S. law, and that the relationship between the user and Linden Lab will be governed in all respects by the laws of the State of California. However, the research report concludes that although Second Life creator and operator Linden Lab is located outside of Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) is applicable to its Canadian activities, stating that PIPEDA applies "to every organization in respect of personal information that the organization collects, uses, or dis-



Global Privacy Dispatches

closes in the course of commercial activities."

Further, in *Lawson v. Accusearch*, the Federal Court determined that PIPEDA gives the Privacy Commissioner of Canada jurisdiction to investigate complaints relating to the transborder flow of personal information (PI). In addition, Second Life is conducting a commercial activity and it collects and uses PI for commercial purposes.

The report also provides a detailed overview of how Linden Lab's Terms of Service and Privacy Policy map to the requirements of the CSA Model Code for the Protection of Personal Information, included in PIPEDA Schedule 1.

Application of PIPEDA Schedule 1 principles

Principle 4.1: Accountability

Linden Lab provides contact information for their legal department in the form of e-mail and mailing addresses.

Principle 4.2: Identifying purposes

Linden Lab states in its Privacy Policy that it collects PI and usage statistics to maintain a high-quality customer experience and deliver superior customer service. The Terms of Service state that PI is used to operate and improve Second Life and to learn what the user likes. "Personal information" is defined by Linden Lab to mean "any information that may be used to identify an individual, including, but not limited to, a first and last name, home or other physical address, an e-mail address, phone number, or other contact information, whether at work or at home."

Principle 4.3: Consent

By clicking “I agree” to the Terms of Service at the time of registration, the user agrees to its conditions. The Privacy Policy states that the use of the Linden Lab Web sites and/or any Linden Lab products or services signifies the user’s assent to the Privacy Policy. Users outside of the U.S. are also made aware that PI may be stored and processed in the U.S. or any other country in which Linden Lab maintains facilities, and by using these Web sites, the user consents to such information transfer.

Principle 4.4: Limiting collection of personal information

Signing up to Second Life requires new users to input their birthday, real first and last names, gender, country and a valid e-mail address. This information provides the user a “Basic” account. Those wanting to participate in Second Life’s economy must obtain a “Premium” account, for which they must provide a valid credit card and address.

To access adult content, users are required to prove that they are at least 18 years old and must provide their name, date of birth, and address. American residents are asked to provide the last four digits of their Social Security number. Non-U.S. residents may be required to provide other documents depending on their country of residency, such as a passport, driver’s license, or national ID number.

The report assumes that Linden Lab collects users’ IP addresses. Linden Lab does not consider IP addresses to be personally identifiable, but the federal privacy commissioner has determined that an IP address can constitute personal information under PIPEDA if it can be associated with an identifiable individual.

Principle 4.5: Limiting use, disclosure, and retention of personal information

The Terms of Service lists situations in which Linden Lab will disclose PI, such as fulfilling a user’s service request, or for customer support, billing, and credit-verification services. The Terms of Service also authorize Linden Lab to dis-

close any information about users to private entities, law enforcement agencies, or government officials when the company feels it is “necessary or appropriate to investigate or resolve possible problems or inquiries, or as otherwise required by law.”

Principle 4.6: Accuracy of personal information

In its Privacy Policy, Linden Lab states that users will have the ability to update the personal data provided to them during registration by contacting Linden Lab via e-mail. However, it does not appear that Linden Lab allows users to update the personal information that has been collected outside of the registration process.

Principle 4.7: Safeguards

In its Privacy Policy, Linden Lab claims to comply with applicable laws and industry standards when transferring, receiving, and storing consumer data. Access to users’ PI is limited to Linden Lab employees who need the information in order to provide products or services or to perform their jobs. The Terms of Service, however, state that Linden Lab does not guarantee the security of any user’s private transmissions against unauthorized or unlawful interception or access by third parties.

Principle 4.10: Challenging compliance

Linden Lab published its legal department’s e-mail address in the Terms of Service and Privacy Policy for questions and comments surrounding privacy and provided its mailing address in San Francisco.

“The OPC report argues that this data classifies as ‘personal information’ under Canadian privacy legislation”

The avatar and the person behind the avatar

Linden Lab collects certain user information, such as the extent of play, time of play, and connection location, as well as the social and economic activities users engage in. The OPC report argues that this data classifies as “personal information” under Canadian privacy legislation. Second Life residents may feel that their online conduct is anonymous and may engage in activities on the assumption that their real-life identity would not be linked to their online identity, but Linden Lab has the ability to link both.

Business practices on Second Life

The OPC researcher notes that organizations that set up on Second Life to conduct business should comply with fair information practices if they collect PI from their employees, customers, or clients on Second Life.

The OPC report also notes that there are still many unanswered questions about privacy in online worlds such as Second Life, and that sites will likely raise new and more questions regarding the applicability of real-world law to virtual world activities. It concludes with questions:

- How might Canadian privacy legislation apply to Canadian businesses and organizations that choose to establish a presence on Second Life?
- PIPEDA aside, what general data practices are recommended to protect the privacy of their clients and customers in Second Life?

For the full research results visit: www.privcom.gc.ca.

Terry McQuay, CIPP, CIPP/C, is the founder of Nymity, which offers Web-based privacy support to help organizations control their privacy risks. Learn more at www.nymity.com.

See, [Global Privacy Dispatches](#), page 12

Global Privacy Dispatches*continued from page 11***FRANCE***By Pascale Gelly and
Elisabeth Quillatre***CNIL watching video surveillance system**

A video surveillance system has been installed in Lille city buses in northern France. The system records images and sounds continuously in order to improve driver and passenger safety.

*Pascale Gelly*

Only police can access the audio and video footage, and the recordings are deleted after a period of 48 hours.

The bus company notified the French data protection authority, CNIL, of the surveillance before implementing. CNIL responded that that the system should not be implemented, as continuous recording would be disproportionate to the purpose of the system and, therefore, not justified. The authority suggested that recording could be triggered by the bus driver in the instance of an assault or other event. CNIL officials followed up with an unannounced onsite investigation in May 2008.

This is a first-stage opinion from the CNIL. The bus company will appear before the CNIL this month to analyse the results of an audit. The CNIL will then render a final decision.

Illicit content reporting platform

The French Ministry of Interior has introduced a new Web site called www.internet-signalement.gouv.fr that lets Internet users report illegal Internet content or behavior.

The site follows the creation of www.signal-spam.fr, for reporting spam, and www.mediateurdunet.fr for private or commercial controversy.

Appropriate use of the platform requires that the content being reported

is prohibited and punishable by French law. It must also be public in the sense that any user could find it. Once such content is reported, police officers proceed to its legal characterization. If the police consider the content illicit, and if it has been created in France, a criminal investigation may be opened under the authority of the public prosecutor. If the content has been created in a foreign country, the case will be forwarded to Interpol, which will redirect it to the judicial authorities of the concerned country.

The platform FAQs state clearly that the tool must not be used to report private disputes, and that any malicious reporting of facts known to be untrue is subject to criminal sanctions and will be prosecuted. When Internet users fill in the reporting form, they have the option of identifying themselves or remaining anonymous. However, their IP addresses are collected in either case. If necessary for the purposes of the investigation, authorities can request Internet service providers to disclose information about the holder of the IP address, but only after obtaining the permission of a public prosecutor.

Approximately 299,005 Internet users had logged onto this platform 45 days after it launched in January and 7,267 suspicious cases have been identified. The French Minister of Interior welcomed this outcome, stating in *Le Figaro* that the "Internet has become the favourite playground of criminals of all kinds."

Air France tests biometrics for autonomous boarding

Air France began testing what could be part of "the airport of the future" on March 17. The smartboarding® card, enables autonomous boarding and is available for frequent Paris-to-Amsterdam travellers to test on a voluntary basis.

To do so, the customer must create his smartboarding® card, which includes an RFID chip (radio frequency identification) containing the customer's name and surname, his/her frequent traveller identification number, and the encrypted fingerprint template

"The smartboarding card contains three technologies: biometrics, RFID, and thermal printing."

of his/her index finger.

To obtain the boarding pass, the customer introduces his/her smartboarding® card in the terminal, and the departure management system verifies the coded identification information. The passenger then receives his card with flight and booking information printed on the back.

Then, at boarding time, the passenger passes through a portico where a control compares the device fingerprint to that stored on the card.

Thus, the smartboarding® card includes three types of technologies: biometrics (for the fingerprint template encrypted on the chip), RFID (dialogue within a short distance using radio waves), and the technology of thermal printing (rewritable up to 500 times).

Since the system involves the automated processing of personal data based on the recognition of fingerprints to control passengers boarding an aircraft, Air France has requested the prior authorisation of the CNIL in compliance with the French data protection law. During a deliberation in June 2008, the CNIL decided to authorize the implementation of this processing (deliberation 2008-179). The CNIL noted that only the personal data of volunteers would be processed and that the fingerprint template would be stored only on an individual media owned by the data subject (as opposed to centralized database).

Shops and stores: simplification of formalities

According to the French Data Protection Act, the processing of personal data relating to offences is subject to prior authorization by the CNIL since

such data is considered sensitive.

As a consequence, business victims of offences such as fraud or theft can collect and process data about offenders only after having obtained authorization from CNIL, which can be a lengthy process.

The CNIL has decided to simplify this process for shops and stores by issuing a so-called "Unique Authorization." By acknowledging on the CNIL Web site that they comply with the data processing conditions set by the authority, applicants are automatically authorized to launch their processing.

Several conditions must be met to benefit from this simplified procedure:

- the commission of the offence can be recorded only if it took place inside a store;
- the processing should target only the management of dispute or litigation; data must be limited to identification data, contact details, and information about prior claims, which means that sensitive data (such as ethnic and racial origin, political opinions, religion beliefs, etc.) cannot be collected;
- the information should be kept only as appropriate under French law (i.e. applicable statute of limitation or the end of court proceedings); the deletion of data beyond this period guaranteeing a "right to oblivion;"
- the recipients of the data processing are also restricted: legal services and security services of the company, as well as judicial authorities;

"Where the Unique Authorization conditions are not met, the data controller will have to provide a detailed description of the system..."

- other "usual" data protection obligations must be complied with, such as the notice to data subjects, security and confidentiality of data, mechanism to exercise rights of access and rectification.

Where the Unique Authorization conditions are not met, the data controller will have to provide a detailed description of the system in its request for CNIL prior authorization.

Theft of the French president's bank details

It all started when President Nicolas Sarkozy found that 170 Euros had been charged on his bank account for no reason. The police investigated, suspecting something big planned against the president. In the end, it turned out that an employee of a subcontractor for Canal +, the French pay TV channel, who had access to customer data, forwarded the bank details of several Canal + subscribers (including the President) to his accomplices who were responsible for the rest of the scam, which totalled 30,000 to 40,000 Euros.

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

THE NETHERLANDS

By Richard van Staden ten Brink

Protecting children on the Internet

Dutch data protection law provides that the consent of a parent or legal guardian is required to collect personal data from children under 16. Until recently, this provision was rarely enforced. However, it appears that the Dutch Data



Richard van Staden ten Brink

"The investigation showed that 71.6 percent of the members were younger than 16."

Protection Authority (DPA) is now actively targeting Web sites that collect children's personal data.

On March 24, the DPA published two decisions regarding such Web sites. One decision concerned the site Jiggies.nl, where members could opt-in to receive commercial e-mail and get so-called "jiggies" in return. If enough "jiggies" were collected, members could exchange them for money. A game on the site—Jiggy Coco Banana—persuaded visitors to become members.

The DPA's primary objection against the site was that it did not verify whether a new member was 16 or older and did not warn children less than 16 years of age to ask their parents for consent. After a forensic investigation and several discussions between the DPA and the Web site owner, the owner modified the site to prevent children from becoming members.

The second site that came under DPA scrutiny was a social network called zikle.nl. The Web site owners had indicated in a magazine interview that the site was targeted at 10- to 15-year old children. A forensic investigation of the site showed that it did not verify whether a new member was 16 or older and did not warn children under 16 to ask their parents for consent. The investigation also showed that 71.6 percent of the members were younger than 16. After several discussions with the DPA, the Web site owner modified the site.

Now, on the membership application form children less than 16 years of age must declare that their parents have given them permission to become a

See, Global Privacy Dispatches, page 14

Global Privacy Dispatches

continued from page 13

member. Apparently, the DPA did not require the owners of zikle.nl to verify the parent’s consent in any way.

Richard van Staden ten Brink is advocaat at De Brauw Blackstone Westbroek. He may be reached at richard.vanstadentenbrink@debrauw.com

“P1000 sent two more messages to Pasternak after the enactment of the Anti-Spam Act...”

ISRAEL

By Dan Or-Hof, CIPP

First Anti-Spam Act decision delivered

For the first time in Israel, a Web site will pay damages under the new spam act. On April 2, a small-claims court in the city of Rehovot ordered P1000, an e-commerce Web site, to pay NIS2,000 (about \$500) in statutory damages for sending unsolicited commercial e-mail messages without receiving prior explicit and written consent.



Dan Or-Hof

The court's decision follows the enactment of Amendment No. 40 to the Communications Act—the Anti-Spam Act—in December of last year. Under the Act, failure to comply with a strict

opt-in regime may result in NIS1,000 in damages per message received. Violations may also result in class actions and administrative fines of up to NIS202,000 (about \$50,000). In 2008, the plaintiff, Mr. Elihay Pasternak, received 60 commercial e-mail messages from P1000, despite his repeated requests for removal of his details from the Web site’s contact list. P1000 sent two more messages to Pasternak after the enactment of the Anti-Spam Act, and the court ordered the maximum damages for each message sent.

The decision can be viewed at: http://www.law.co.il/media/computer-law/pasternak_p1000.pdf (Hebrew only).

Dan Or-Hof is a senior counsel at Pearl Cohen Zedek and Latzer LLP, with specific expertise in data protection and privacy law. He may be reached at dano@pczlaw.com.

**practical
privacy**
● ● ● *series*

Register Now
www.privacyassociation.org



Silicon Valley, CA

REAL SOLUTIONS FOR BUILDING BEST PRACTICES

WEDNESDAY, 17 JUNE

-  Data Breach
-  Data Governance

THURSDAY, 18 JUNE

-  Human Resources
-  IT Security and Privacy



Facebook: the future of service of process?

By Nick S. Pujji, Anahit Tagvoryan, and Joshua M. Briones at law firm DLA Piper in Los Angeles

Recent developments regarding the service of process via social networking Web sites provide insight into the ways the Internet and technology continue to shape the practice of law.

Facebook, a popular social networking Web site, currently has more than 200 million active users worldwide. Many users of Facebook and similar Web sites join to network, keep in touch with family and friends, or just for entertainment. However, recent developments suggest that the implications to an online presence may be quite far reaching. It appears that courts outside the United States are increasingly allowing formal court documents to be served via Facebook, and U.S. courts have already admitted evidence obtained from online profiles in court proceedings.

What implications does this have on the practice of law—especially for litigation in the U.S.?

Courts in Australia and New Zealand approve service of process via Facebook

Courts in at least two countries have already allowed legal documents to be served via Facebook. The Australian Capital Territory Supreme Court, for example, allowed formal court papers that gave notice of default on a loan to be served on two individuals via Facebook. The Supreme Court granted the attorney's request to serve the documents after several failed attempts to personally serve the individuals at home and by e-mail. The Supreme Court



Nick S. Pujji



Anahit Tagvoryan



Joshua M. Briones

agreed that the method of service was a reliable and valid way to provide notice after the party's attorney demonstrated that the information the individuals had provided to the lender matched the information in the individuals' profiles on Facebook.

Similarly, the New Zealand High Court allowed a man to be served with process in a case involving failed business dealings. The New Zealand plaintiff's lawyer argued that the defendant's exact whereabouts were unknown, but demonstrated that the potential defendant maintained a social presence on Facebook.

Current U.S. jurisprudence

While there is no record yet of courts in the U.S. allowing formal service via Facebook, prosecutors are commonly permitted to use photographs obtained from social networking Web sites as evidence in court for a variety of proceedings—from divorce to sexual harassment to drunk driving to murder cases.

Federal Rule of Civil Procedure 4(e)(2)(B) allows an individual located within a U.S. judicial district to be served by leaving documents at an

"individual's dwelling or usual place of abode..." While the terms "dwelling or usual place of abode" are understood to mean an individual's physical home, it is not unrealistic to predict that this language could one day be expanded by a court to include a person's usual place of virtual abode.

Furthermore, Federal Rules of Civil Procedure 4(f)(2) and 4(f)(3) allow an individual located in a foreign country to be served, in the absence of internationally agreed means, "by a method that is reasonably calculated to give notice...as prescribed by the foreign country's law for service" or "by other means not prohibited by international agreement, as the court orders." This language clearly allows room for the service of process via social networking Web sites on individuals who are outside of the U.S. It certainly allows service on individuals located in Australia and New Zealand, if a reasonable case can be made.

Implications in the U.S.

The materials and photographs that become a part of an individual's online profile are already being used as admissible evidence in U.S. courts. Will the ability to serve process via the virtual world be the next milestone? The implications of this possibility are considerable. Many Facebook users joined the Web site for fun and amusement or to more easily keep in touch with family and friends. Their membership, however, may also make them more accessible to the legal system. Professional process servers may soon no longer be required to play cat-and-mouse games in the physical world in order to personally serve individuals.

In light of these potential legal ramifications, online users would do well to rethink the content and accessibility of their own online profiles as well as the legal implications of new technology generally.

"The implications of this possibility are considerable."

knowledge net

What keeps you up at night?

On a recent Wednesday, 35 privacy pros gathered at Ernst & Young's Boston offices for lunch and a panel presentation on the topic "What's Keeping You Awake at Night in 2009?" Presenters included Joan Quinn, privacy compliance and risk executive at Bank of America and Boston KnowledgeNet co-chair; Jeannette Frey, Fallon Community Health Plan privacy officer; and David Szabo, partner and privacy attorney with the law firm of Nutter McClennen & Fish. Mike Spinney, SixWeight principal and Boston KnowledgeNet co-chair, served as moderator.

A lively discussion transpired, with panelists fielding many insightful questions on issues ranging from the impact of new legislation, to dealing with social networking utilities and the affect of a new tech-savvy presidential administration.

The topics that generated the most vigorous discussion included:

Massachusetts data protection regulations "201 CMR 17:00 Standards for the Protection of Personal Information of Residents of the Commonwealth"

Although there was optimism that attendees' individual organizations would be in compliance, the detailed, prescriptive nature of the law's multiple provisions, along with a lack of definition on some of the key terms, has generated more work for those falling under the law's provisions, and has raised concerns about how the regulations will be interpreted and enforced by the Commonwealth.

(See the regulations online at: [/www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf](http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf))



(L to R) Mike Spinney, David Szabo, Jeannette Frey, Joan Quinn, Junaid Hoosen, Sr. Manager of Assurance and Advisory Business Services at Ernst & Young LLP; and Web Hull, Sr. Privacy & Compliance Specialist at Iron Mountain and Boston KnowledgeNet Co-chair.

Complexity of cross-border data transfers

Companies that have operations or outsourced functions in multiple nations continue to devote a significant amount of effort to managing all of their data protection obligations in and among the various countries.

"The ARRA significantly increases the obligations of healthcare industry's 'business associates...'"

Privacy impact of the recession

With companies contracting, folding, or being acquired, personally identifiable information may be managed by fewer people or moved to new custodians, potentially increasing the risk of breach and creating new challenges for privacy pros in charge of management and compliance.

Privacy requirements of the stimulus bill

The American Recovery and Reinvestment Act of 2009 (ARRA) significantly increases the obligations of healthcare industry's "business associates" to enhance their protected health information safeguards. Some expressed concerns that a number of current business associates might simply exit the sector rather than exert the effort required to meet the new requirements. (See a copy of the ARRA at: <http://fdsys.gpo.gov/fdsys/pkg/BILLS-111hr1ENR/pdf/BILLS-111hr1ENR.pdf>.)

In a concluding general discussion, participants agreed that, as a nation and profession, we are heading into a period of significantly increased regulation and enforcement.

KnowledgeNet events will be held in Denver and Austin in the coming weeks. See page 18 for details.

What are you reading?

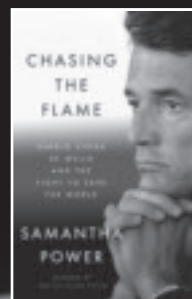
The *Privacy Advisor* asked Greg Pemberton what he is reading these days. Here's what Greg had to say:

"Chasing the Flame is a biography of longtime United Nations staffer Sergio Viera de Mello. Though this is not a 'privacy' book, there are many things to learn, or at least observe, from de Mello's methods. He was a larger-than-life character and a very human and flawed hero who often chose assignments in highly unstable and violent regions. He rose to the upper ranks of the UN steadily until his unfortunate and untimely death in Baghdad in 2003, when a suicide bomber targeted the UN headquarters. His legacy lives on in this book, a documentary film due out this year, and through a new campaign called Chasing The Flame."

Brief preview: <http://books.google.com/books>



This month's reader:
Greg Pemberton,
Privacy Specialist and
Database Administrator
Dalhousie University,
Halifax, Nova Scotia



What Greg is reading:
*Chasing the Flame: One
Man's Fight to Save the
World*
By Samantha Power
Penguin Press, 2008



In the *Privacy Tracker* this month...



MAY 2009

After years of debate and little progress, recently passed economic stimulus legislation has ushered in a new era for healthcare privacy and security. In the American Recovery and Reinvestment Act of 2009, Congress created a wide range of new incentives for healthcare providers to develop and utilize electronic medical records. In anticipation of the move toward widespread health IT, the Health Information Technology for Economic and Clinical Health (HITECH) Act creates added privacy protections for HIPAA-covered and non-HIPAA-covered healthcare providers.

In this month's *Privacy Tracker* newsletter, Wiley Rein partner Kirk J. Nahra discusses the changes and explains that healthcare companies across the board must pay close attention to the new rules and begin developing strategies to meet the requirements. A substantially stronger enforcement environment is on its way.

Subscribe to the *Privacy Tracker* suite today to begin receiving monthly printed newsletters, weekly legislation-tracking updates, access to regular calls with leading privacy experts, and access to the *Privacy Tracker* Web site.

www.privacytracker.org



Did You Know?

2010 COPPA REVIEW

The U.S. Federal Trade Commission will expedite its review of the Children's Online Privacy Protection Act to determine whether it needs updating based on the increasing use of smartphones for accessing the Web. The review was scheduled for 2015, but will take place next year.

Source: FTC

LOST LAPTOP = EXPENSIVE LAPTOP

After adding costs associated with the investigation, lost productivity, fraud prevention, and more, the typical stolen or lost laptop costs a company nearly \$50,000.

Source: Ponemon Institute

STANDARDS, PLEASE

Six in 10 consumers endorse government establishment of standards for how medical information is collected, stored, and exchanged.

Source: Deloitte 2009 Survey of Health Care Consumers

APPLICANTS WANTED

The Department of Homeland Security Privacy Office is seeking applicants for the DHS Data Privacy and Integrity Advisory Committee. For application details visit: www.dhs.gov/xinfo/share/committees/editorial_0512.shtm. Deadline to apply is June 8.

Source: U.S. DHS



Calendar of Events

MAY

- 13 IAPP KnowledgeNet – Tel Aviv, Israel**
9 - 11:30 a.m.
Speakers: Steven C. Bennet, Partner, Jones Day, New York; Dr. Omer Tene, Associate Professor, College of Management School of Law
Topic: Information Privacy Aspects of E-Discovery
- 18 IAPP Certification Testing – Denver, CO**
Certification Foundation, CIPP, CIPP/G and CIPP/C
- 20 IAPP KnowledgeNet – Denver, CO**
11:30 a.m. - 1 p.m.
Speaker: David Navetta, JD, CIPP, InfoSecCompliance, LLC
Topic: Hot Topics in InfoSec and Privacy Law 2009
- 26 IAPP Certification Testing – Orlando, FL**
Certification Foundation, CIPP, CIPP/G and CIPP/C
- 28 IAPP KnowledgeNet – Austin, TX**
11:30 a.m. - 1:30 p.m.
Speaker: Charisse Castagnoli, Independent Security Consultant & Lecturer
Topic: Overview of the Emerging Web Cyber Threats Resulting in Increased Identity Theft

JUNE

- 1-4 Computers, Freedom, and Privacy 2009 Conference**
Marvin Center, George Washington University
Washington, DC
<http://www.cfp2009.org>
- 5 New Data Security Rules and Best Practices**
8:30 a.m. - 12 p.m.
Suffolk University Law School, Boston,
www.law.suffolk.edu/academic/als/course_detail.cfm?cid=651

- 15 IAPP Certification Testing – Washington, DC**
Certification Foundation, CIPP, CIPP/G and CIPP/C
- 17-18 Practical Privacy Series: Data Breach, Data Governance, Human Resources, Information Security**
Santa Clara, CA
- 18 IAPP Certification Testing – New York, NY**
Certification Foundation, CIPP, CIPP/G and CIPP/C
- 19 IAPP Certification Testing – Santa Clara, CA**
Certification Foundation, CIPP, CIPP/G and CIPP/C

JULY

- 3 HP-IAPP Privacy Innovation Award Nominations Deadline**
www.privacyassociation.org/
- 24 Goodwin Procter-IAPP Privacy Vanguard Award Nominations Deadline**
www.privacyassociation.org/

SEPTEMBER

- 17 Privacy Dinner**
Boston, MA
- 16-18 Privacy Academy 2009**
Boston, MA

DECEMBER

- 8 Practical Privacy Series: Government**
Washington, DC

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

Congratulations, certified professionals!

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



Clark Douglas Asay, CIPP	Olya Pestova, CIPP	David Edward Baker, CIPP
Jordi Batlle, CIPP/IT	Jeffrey John Roby, CIPP	David Baldwin, CIPP
Matthew Scott Beebe, CIPP	Christine Marie Santariga, CIPP	Lisa Edith Branner, CIPP
Michael Cen, CIPP	Raghu Bryan Seshadri, CIPP	Kirk Dean Darbe, CIPP
Patrick Edward Cox, CIPP	Kenneth Edward Washington, CIPP	Alok N. Mathur, CIPP
Virginia Downie, CIPP	William Henry Mohr, CIPP	David Isaac Morgan, CIPP
Brian Eng, CIPP	Samuel Shlozberg, CIPP	Barbara A. Hazzard, CIPP/G
Larry Robert Fasching, CIPP	Bonnie Lee Yeomans, CIPP	Mark Gerard Masone, CIPP/G
Julie Ashworth Glover, CIPP	John S. Baur, CIPP	Belinda Miller, CIPP/G
James Thomas Graves, CIPP	Peter David Bernstein, CIPP	Frederick J. Sadler, CIPP/G
Karen T. Green, CIPP	Pamela Joyce Carcirieri, CIPP	Emma Jane Sutcliffe, CIPP/IT
Renee Josephine Guttman-Stark, CIPP	Sylvia C. Diaz, CIPP	John Howie, CIPP/IT
Suzanne Carrie Lieberman, CIPP	Andrew Joseph Espinoza, CIPP	Aaron Keith Weller, CIPP/IT
Kristin Wontka Longo, CIPP	Lisa A. Hammond, CIPP	
Eric Howard Lybeck, CIPP	Sybill Michelle McDowell, CIPP	

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

If you are a recent CIPP, CIPP/G, CIPP/C or CIPP/IT graduate but do not see your name listed above then you can expect to be listed in a future issue of the Privacy Advisor. Thank you for participating in IAPP privacy certification!

Privacy Classifieds

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

PRIVACY OFFICER
USDA, Food Safety & Inspection Service
Washington, DC

PRIVACY ANALYST
U.S. Department of the Treasury
Washington, DC

COMPLIANCE ANALYST, OFFICER
State Street Corporation
Boston, MA

DIRECTOR OF INFORMATION SECURITY
Qwest Communications
Denver, CO

PRIVACY COUNSEL
Vodafone
Newbury, UK

SENIOR POLICY MANAGER, PRIVACY
Yahoo!
Sunnyvale, CA

PUBLIC AFFAIRS: ASSOCIATE DIRECTOR FOR COMMUNICATIONS
U.S. Department of Homeland Security
Rosslyn, VA

PRIVACY ANALYST
U.S. Department of Homeland Security
Rosslyn, VA

PRIVACY OFFICER
State of California Department of Industrial Relations
San Francisco, Sacramento, or Los Angeles, CA

SECURITY AND DATA PRIVACY ANALYST
SVB Financial Group
Santa Clara, CA

We're looking for a few good innovators

Submit your nomination for the 2009 HP/IAPP Privacy Innovation Award

Nominations are now being accepted for the organizations that have demonstrated the most effective integration of privacy programs in 2009.

Winners will be announced in three categories:

- large organization (more than 5,000 employees)
- small organization (fewer than 5,000 employees)
- most innovative technology

Awards will be presented at the IAPP Privacy Dinner 2009, 16 September in Boston.

For more information, visit
www.privacyassociation.org



Employee monitoring

continued from page 7

or expected to engage in monitoring to the same extent. In addition, the use of monitoring technology across borders may trigger specific compliance obligations in certain countries. For instance, in the case of deployment of such tools on the systems of an international company with European subsidiaries or branch offices, there may be a need to implement standard contractual clauses or alternative means of justification for the transfer of personal data between the European subsidiary and the non-European parent.

Companies can avoid many legal conflicts and can maximize the extent of visibility into their employee's IT use within the limits of the law by selecting, deploying, and configuring monitoring technologies and implementing related policies on a country-by-country basis. To what extent this is feasible will depend in part on the way in which the company network is set up. Suppliers of monitoring technologies, on the other hand, can support this effort by designing the relevant tools in a manner that enables such differentiation. In light of international legal trends in the regulation of employee monitoring, it is likely that providers of customizable solutions allowing employers to monitor to the greatest extent permissible in each jurisdiction will have a competitive edge over suppliers of (would-be) one-size-fits-all solutions.

Lothar Determann is a partner in the technology practice group of Baker & McKenzie LLP, San Francisco/Palo Alto office (www.bakernet.com) and teaches Computer and Internet law at the University of California Berkeley School of Law (Boalt Hall), University of San Francisco School of Law, and Freie Universität Berlin (www.lothar.determann.name).

Lars F. Brauer is an associate in the same practice group.

The IAPP Welcomes our Newest Corporate Members



Yahoo Inc.



**2nd Story
Software Inc.**

**USCIS
Verification Division**
Department of
Homeland Security

Apple



ID Watchdog, Inc.



MetLife



Privacy News

TRUSTe acquires Haute Secure

Privacy trustmark provider TRUSTe has acquired Haute Secure. Haute Secure develops Web site scanning and anti-malware technology. The purchase allows TRUSTe to expand its services; among other additions, the company will begin offering reputation and anti-malware scanning services for browsers, Web sites, and online communities.



"...Ultimately, this is about giving people a sense of confidence—that they can trust the Web site, and by extension, the company behind it," said TRUSTe CEO Fran Maier.

www.truste.org

OPC publishes DPI research

The privacy commissioner of Canada has released a series of essays on the subject of deep packet inspection. The essays are intended to give Canadians more insight into a method that the Office of the Privacy Commissioner (OPC) has received a number of complaints about. "Technology can often be beneficial," OPC Director of Research, Education and Outreach Colin McKay told *CBC News*, "but sometimes you do have to be, if not critical, at least questioning to make sure...the technology really is positively affecting your life." The essays present an array of perspectives.



Canadian Privacy Commissioner
Jennifer Stoddart

Essay titles:

- Just Deliver the Packets
- DPI as an Integrated Technology of Control—Potential and Reality
- Deep Packet Inspection: Its Nature and Implications
- Objecting to Phorm
- Transport and Tracking
- DPI: The Future is Out There
- Phorm: A New Paradigm in Internet Advertising
- Deep Packet Inspection and the Transparency of Citizens
- The Privacy Implications of Deep Packet Inspection
- Net Neutrality and Deep Packet Inspection: Discourse and Practice
- The Greatest Threat to Privacy
- Deep Packet Inspection—Bring It On
- Deep Packet Inspection is Essential for Net Neutrality
- Badware and DPI

<http://dpi.priv.gc.ca/> (English)
http://iap.priv.gc.ca (Français)

Wolf joins Hogan & Hartson

Christopher Wolf has joined Hogan & Hartson's Washington, DC office as a partner. Wolf will co-chair the firm's privacy group. The move comes after 20 years as a litigation partner at Proskauer Rose.



Christopher Wolf

More recently, Wolf co-founded the Future of Privacy Forum—a think tank for privacy and security issues. He will continue to be involved with the forum.

Curran heads NAI

Charles Curran is the new executive director and general counsel of the Network Advertising Initiative (NAI). Curran joins the organization after a 12-year stint as AOL's chief counsel for policy and regulatory matters. Before AOL he was a trial attorney for the U.S. Department of Justice.



Charles Curran

The NAI membership includes tech giants such as Google and Yahoo. Curran assumes the helm as the Federal Trade Commission takes an increasing interest in online advertising practices such as behavioral targeting.

"I'm excited to be joining the NAI at this incredibly dynamic time in the public policy discussion of online behavioral advertising," said Curran, who is based in Washington, DC.

NAI Board Chairman Robert Gratchner said Curran's experience in government policy and online advertising suits the NAI well.

New privacy blogs

Two new privacy blogs have entered the sphere.

THE COGITATIO PRIVATIM BLOG features regular postings from Camouflage Software's recently CIPP/C-certified Director of Privacy Research David Morgan.



www.datamasking.com/blog

The Victoria, Australia Department of Justice launched its PRIVACY NOW blog, which is available only to Victorian government employees currently, but privacy pros can follow it on Twitter. Likewise, if you don't have access but have an idea for a PRIVACY NOW post, e-mail Brent.P.Carey@justice.vic.gov.au. <http://twitter.com/PrivacyNow>.

VLRC on CCTV

"Surveillance affects all Victorians, whether we are shopping, catching public transport, driving on major roads, or attending a sporting event,"

The use of closed-circuit television cameras (CCTV) in public places has grown rapidly in Melbourne and other areas of Australia, prompting the Victorian Law Reform Commission (VLRC) to propose regulations on its use.

"Surveillance affects all Victorians, whether we are shopping, catching public transport, driving on major roads, or attending a sporting event," said VLRC chairperson Neil Rees.

The VLRC proposes reforms for surveillance in public spaces. The commission is seeking public feedback on the proposals. Download the paper here: www.lawreform.vic.gov.au/

AEPD releases 2008 report

Claims rose 45 percent over previous year



Artemia Rallo

The director of the Spanish Agency for Data Protection (AEPD), Artemia Rallo, has released his annual report for 2008. The agency filed 2,362 claims in 2008, an increase of 45 percent over 2007 figures. The sectors garnering the highest number of claims were telecommunications, financial, and video. Complaints related to Internet search engines saw the biggest increase overall.

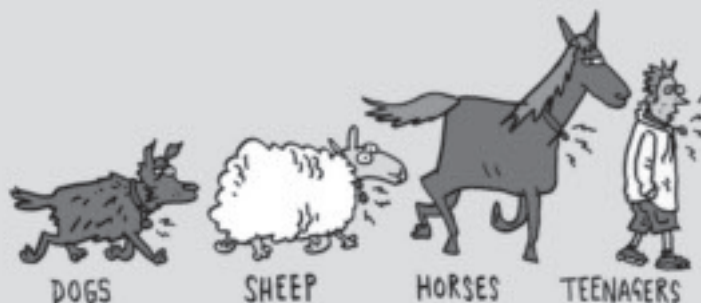
Director Rallo emphasized that the Internet and video are becoming major challenges in protecting citizens' privacy and acknowledged that the video issue is an "unstoppable phenomenon." The agency intends to crack down on the improper posting of videos to YouTube and has already issued two sanctions related to posting videos without the consent of videos' subject(s).

OTHER FINDINGS:

- Among decided claims, 630 resulted in punishment, with 535 of those resulting in fines
- The agency levied €22.6 million in fines in 2008, an increase of 15 percent over the previous year
- The number of complaints surrounding videos tripled to 365
- 75 percent of sanctions were classified as "serious," 18 percent "mild," and seven percent "severe"
- The agency received more than 72,000 queries about how to prevent unsolicited ads via fax or SMS

The Lighter Side of Privacy

MICROCHIPS - THE TREND



Reprinted with permission from Slane Cartoons Limited.

SLANE



IAPP members:

Does your organization offer free or discounted products or services to other IAPP members?

If so, let them know!

Advertise at a DISCOUNTED RATE here in our new member-to-member benefits section.

Contact Wills Catling at
wills@privacyassociation.org
or +1.207.351.1500, ext. 118



MEMBER to MEMBER Benefit

Debix Is The Only Data Breach Solution That's Proven To Work.



Since August 2007, Debix has stopped over 1,400 identity theft attacks.

Debix Breach Solutions Include:

- The only electronic identity theft network
- The industry's best price
- \$25,000 of identity theft insurance
- Breach Response Specialists
- Weekly and monthly reporting.

Sign up for your free year of protection.* Go to www.Debix.com/iapp

To learn more about Debix Breach Solutions, call 800-965-7564 or go to www.debix.com/breach

*Offer limited to registered IAPP Members.



Learn the latest on privacy
without ever leaving your office.

Visit the IAPP's online Educational Library.

FEATURED AUDIO CONFERENCE



**Privacy Training Today:
Thinking Smart and Working Economically**

Developing a cost-effective privacy training program is essential. Learn how to work with an increasingly limited budget, avoid costly mistakes and implement successful strategies.

**Buy it today at
www.privacyassociation.org/edulibrary**

Earn CPE credits while you learn!

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

