Wellness programs and medical inquiries

Many employers are offering wellness programs to employees in an effort to reduce overall health insurance spending and to reduce employee absence due to illness. Typical offerings include exercise, weight reduction, and stress management programs.

Employee participation is, of course, key to the success of these programs and their positive impact on the company’s bottom line. Incentives directly impact employee participation. However, the use of incentives can raise legal issues as well as complaints from employees who may not qualify for the incentives.

Some employers offer incentives in the form of cash payments, days off, reduced health insurance premiums, waived deductibles, and health coaches. In return, employees may be asked to complete an annual health exam, fill out a questionnaire, undergo biometric screening, attend meetings, or consult with a health counselor.

The provisions of HIPAA (Health Insurance Portability and Accountability Act) impose certain limits on wellness programs. Title I of HIPAA prohibits discrimination on the basis of “health factors” such as medical conditions, disability, claims history, genetic factors, and others. However, HIPAA also contains an explicit exception for certain types of wellness programs.

“Unregulated” wellness programs may be offered without restriction by employers. Such programs provide

Some employers offer incentives in the form of cash payments, days off, reduced health insurance premiums, waived deductibles, and health coaches. In return, employees may be asked to complete an annual health exam, fill out a questionnaire, undergo biometric screening, attend meetings, or consult with a health counselor.

The provisions of HIPAA (Health Insurance Portability and Accountability Act) impose certain limits on wellness programs. Title I of HIPAA prohibits discrimination on the basis of “health factors” such as medical conditions, disability, claims history, genetic factors, and others. However, HIPAA also contains an explicit exception for certain types of wellness programs.

“Unregulated” wellness programs may be offered without restriction by employers. Such programs provide

Spies on staff—German employee surveillance practices under scrutiny

By Flemming Moos

Flemming Moos explores the workplace spying scandals that have rocked German businesses in recent months and have led to a hastened cry for passage of an Employee Privacy Act.

The cat was set among the pigeons when it was revealed last year that the major German retail chain, Lidl, which employs about 53,000 people in the nation, had systematically monitored its employees with hidden cameras. And what seemed to be a regrettable singular case at first glance quickly turned out to be just the first in a series of employee-spying scandals among German companies. Prestigious and well-established businesses such as national rail operator Deutsche Bahn, Airbus, and Deutsche Telekom, Europe’s biggest phone company, all confirmed they had conducted clandestine surveillance on their staff. The companies defended many of these activities as

See, Spying on staff, page 8
The business costs of failing to preserve employees’ privacy are rising. Recent Australian Industrial Relations Commission (AIRC) decisions illustrate this. In two cases, employers were ordered to pay back wages to terminated employees whose privacy had been violated by their employers’ mishandling of human resources issues.

Employers worldwide are being held accountable in new and increasingly complex ways when it comes to data privacy and, as we learn in this month’s article about German companies’ surveillance activities, even an organization’s top executives are not immune to the repercussions of privacy faux pas.

The AIRC decisions and the sanctions levied against Deutsche Bahn and Lidl executives, among others, underscore the importance of handling workplace privacy appropriately.

In this month’s newsletter, we continue our employee privacy series with a look at today’s here-and-now human resources issues, employee monitoring, and how organizations that manage group health plans should prepare for the new regulatory requirements of the U.S. HITECH Act.

On a sunnier note, those of us in the northern hemisphere are enjoying summer and its requisite pursuits—downtime, baseball, books… Since we know many of you enjoy a good read, we polled IAPP members to find out what privacy and non-privacy prose they have stuffed in their beach bags this summer. As you turn the pages, you’ll find out what they are reading, what books have impacted their careers, and what they think you should read. Look for the summer reading “bookmarks” within and, if you like these, join us in book club sessions at the Privacy Academy in September.

J. Trevor Hughes, CIPP
Executive Director, IAPP
1. The programs must promote health five conditions: programs are allowed only if they meet penalties less healthy employees, the level. Because these programs may preventative care by waiving a deductible.

In contrast, programs that offer benefits or impose penalties based on health factors are regulated by HIPAA. Under this type of program, an employee might be offered lower premiums if they do not smoke, if their cholesterol level is, for example, below 200, or if their body mass index is below a certain level. Because these programs may penalize less healthy employees, the programs are allowed only if they meet five conditions:

1. The programs must promote health improvement, not just reward healthy employees. Also, they cannot be a subterfuge for discrimination against people with disabilities.

2. The combined value of all incentives must be less than or equal to 20 percent of the total premium for single employee coverage. The incentive may not affect eligibility for a health benefit.

3. All employees must be made eligible at least once each year.

4. The incentives must be available to all “similarly situated” individuals. Furthermore, if an employee may not be able to meet an eligibility factor due to a medical condition, or doing so is medically inadvisable, then the employer must offer a “reasonable alternative” measure of eligibility (e.g., a low-salt diet as an alternative to low blood pressure readings).

5. Plan materials describing program terms must mention the availability of “alternative standards.”

In addition to these rules, employers should seek legal advice on the data privacy requirements under HIPAA and the ADA, which will apply to any medical information that employees provide while participating in such programs. Also, it is important to get legal advice on the disability discrimination issues that arise under the ADA and state disability discrimination laws. Finally, some wellness programs that offer “medical care” are covered by ERISA (the Employee Retirement Income Security Act), which imposes additional requirements and restrictions.

Despite the legal complexities, many employers believe that wellness programs improve employee health enough to generate significant savings in rewards regardless of health factors, or have no incentives at all. If incentives are offered, they must be so low that an employee’s decision to provide health information would be considered voluntary under the Americans with Disabilities Act. Examples include the reimbursement of fees for joining a health club or a smoking-cessation program, or encouraging participation in preventative care by waiving a deductible.

“In addition to these rules, employers should seek legal advice on the data privacy requirements under HIPAA and the ADA...”
health insurance costs and illness absences.

Employee monitoring
Another evolving area relating to employee personal data is the use of electronic monitoring tools to discover employee theft, fraud, and other types of misconduct in the workplace or on the employer’s computer and communication systems. The following is a very-high-level summary of what is generally allowed and prohibited in the U.S. Additional restrictions may exist under certain state laws. In addition, many types of electronic monitoring are prohibited in the European Union and in countries with similar privacy legislation.

In the U.S., most legislation on electronic monitoring recognizes the rights of employers as property owners, who should be free to observe what employees do while on the employer’s property and while using the electronic resources that the employer has purchased for employees to perform their jobs.

Employers now use electronic devices to conduct monitoring inexpensively, as compared to decades-old efforts involving legions of supervisors and security guards. The tools may be as simple as access systems that record data from an employee’s ID badge as they enter and leave the workplace, or as sophisticated as “content monitoring” software that silently registers activities by all users in the employer’s computer system, then flagging or prohibiting certain behaviors that may indicate misconduct by an employee.

Employees in the U.S. have no general right of privacy in the workplace under the federal Constitution, or under most state constitutions. A few state constitutions create employee privacy rights, and a number of states recognize certain privacy torts. While courts have rarely interpreted either to create significant restrictions on the most typical types of employer monitoring, more recent cases have created some exceptions.

Telephone monitoring
The federal “wiretap” law has regulated telephone monitoring since the mid-twentieth century. Generally, it prohibits the interception of telephonic conversations without the express consent of at least one participant. However, it also recognizes the right of “service providers” to intercept calls in the normal course of providing the service. Employers are often deemed to be providers of their own phone systems, and therefore have a limited right to monitor calls of a non-personal nature. However, it is advisable for employers to obtain consent from its employees to the monitoring of calls. For example, an employer may want to get written consent from employees in a call center as a condition of taking the job. This will allow unlimited monitoring of calls by the employer, except in 12 states that require two-party consent. For calls in those states, or involving individuals in those states, most companies use a pre-recorded notice of monitoring. If the caller stays on the line, they give an implied consent to monitoring.

Video monitoring
Many employers place video cameras at facility entrances, in parking lots, and in

Keith
What privacy book do you wish you had written?
Unwanted Gaze: The Destruction of Privacy in America, by Jeffrey Rosen

(I studied with Jeff when he was writing this and continue to find his writing brilliant, even when I disagree with him. I have an autographed edition of this, and, at this rate, it’ll be worth more than my house soon...)

Telephone monitoring
The federal “wiretap” law has regulated telephone monitoring since the mid-twentieth century. Generally, it prohibits the interception of telephonic conversations without the express consent of at least one participant. However, it also recognizes the right of “service providers” to intercept calls in the normal course of providing the service. Employers are often deemed to be providers of their own phone systems, and therefore have a limited right to monitor calls of a non-personal nature. However, it is advisable for employers to obtain consent from its employees to the monitoring of calls. For example, an employer may want to get written consent from employees in a call center as a condition of taking the job. This will allow unlimited monitoring of calls by the employer, except in 12 states that require two-party consent. For calls in those states, or involving individuals in those states, most companies use a pre-recorded notice of monitoring. If the caller stays on the line, they give an implied consent to monitoring.

Video monitoring
Many employers place video cameras at facility entrances, in parking lots, and in
warehouses or other locations with a higher risk of employee theft. The cost of this technology continues to decrease.

There is no federal law restricting the private use of silent video monitoring. Consequently, an employer may place video cameras in almost any location on its property, without prior notice to employees. Note that in Connecticut and Delaware, employers must post notices of their video monitoring activities before beginning such activities. In addition, New York and a number of other states have laws prohibiting or restricting the use of video in locker rooms, changing rooms, and similar locations. Placing a camera in an employee’s office might create a common-law invasion of privacy claim in California and a few other states if the employee has a reasonable expectation that their office is generally private, and the employer has not notified them of their right to monitor activities in such locations.

E-mail, text messages, and Internet use
In 1986, the wiretap laws were amended by the Federal Electronic Communications Privacy Act to cover the interception of electronic communications, including e-mail. The Stored Communications Act further amended the laws to protect electronic communications in storage on computers. However, these laws continued the exceptions that allow the interception of communications with the consent of one party, as well as the right of “service providers” to monitor communications in their systems.

More specifically, if an employer is the “provider” of the equipment and applications that facilitate e-mail and text messaging, it is free to review any message stored in its systems without prior notice to, or consent from, anyone using those systems. As a result, even if an employer reads an employee’s personal e-mails or texts sent via the employer’s systems, the employee has no claim under federal law. In addition, few state courts have found such activities to violate common law, unless the employer has led an employee to believe that their use of such systems would not be monitored.

The situation is more complicated if an employer uses a vendor to provide e-mail, text messaging, or instant messaging services to employees. In such cases, even if the employer is the “subscriber” to such services, some courts have held that the employer may not compel the vendor to provide copies of an employee’s messages without the employee’s consent. As a result, employers who purchase such services from vendors should obtain a blanket consent from each employee as a condition of using such messaging services. In addition, employer policies should make clear that an employee must consent to any later employer request for copies of such messages in the course of an employer investigation. See, HR privacy issues, page 22

THE IAPP WANTS YOU!

OPT-IN to the 2010 IAPP Membership Directory
www.privacyassociation.org

Sponsorship and advertising opportunities are available for the directory. For information, please contact wills@privacyassociation.org.

Don’t miss out on your chance to be listed in the 2010 IAPP Membership Directory—opt-in today!

Only IAPP members who opt-in will have their names and contact information included in the 2010 edition.

The deadline for inclusion is October 30, 2009.
Group health plans and the HITECH Act

Helping your company meet the new challenges

By Amy E. Yates, CIPP

With little enforcement activity occurring prior to the summer of 2008, many companies governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) paid scant attention to their obligations under the Privacy and Security Rules after the initial flurry of activity in 2003. However, with the enactment of the American Recovery and Reinvestment Act 2009 (ARRA)—which includes provisions related to Health Information Technology (HIT), the Health Information and Clinical Health Act (HITECH Act)—physicians, hospitals, nursing homes, and other healthcare entities will receive grants and payment incentives for adopting and making meaningful use of technology for the creation and management of electronic health records (EHRs). Importantly, the legislation includes significant provisions intended to boost public confidence in the use of EHRs and personal health records by broadening the scope of activities covered by HIPAA, and by increasing enforcement rigor around an entity’s privacy and security obligations. These new requirements for EHRs will significantly impact providers’ record-keeping operations. But the HITECH Act and the refocus on HIPAA should cause all covered entities, including the group health plans of companies, to revisit their HIPAA privacy programs to meet the challenges of this new regulatory environment.

Any company that manages group health plan activities should consider the following actions for bolstering its ability to address the increased HIPAA compliance expectations:

• conduct HIPAA privacy and security assessment;
• refresh HIPAA policies and procedures;
• retrain on HIPAA policies and procedures;
• implement security and privacy incident response program; and
• assess business associates and related activities (including a review of business associate agreements).

Conduct HIPAA privacy and security assessment

Any company that has not conducted an assessment of its HIPAA privacy and security program and group health plan activities in a few years should consider undertaking such an assessment now. Understanding where protected health information resides and what controls have been implemented to secure that data takes on increased importance as the Department of Health and Human Services (HHS) intends to issue annual guidance on technical safeguards. Likewise, identifying whether a company’s group health plan has adequately addressed its obligations around providing individual rights (e.g., access, amendment, accounting of disclosures) and remediating identified gaps would be prudent in light of HHS’s intent to increase its audit activities.

Review and refresh HIPAA privacy and security policies and procedures

In connection with their recent enforcement activities, agencies have cited the “disconnect” between the operations of an entity and its policies and proce-
dures as a material factor in imposing significant penalties. It is critical that HIPAA policies accurately reflect the way an entity uses, discloses, and secures protected health information. Importantly, policies should not cite the HIPAA regulation's chapter and verse. Accordingly, companies should carefully draft policies to describe the manner in which actual business operations function to satisfy HIPAA requirements.

Re-train on HIPAA policies and procedures
Periodic training on the policies surrounding the use, disclosure, and protection of protected health information is important to ensure that employees consistently follow established procedures and understand the importance of protecting such data.

Implement security and privacy incident response program
HITECH's requirement that individuals be notified of security and privacy breaches that impact their protected health information reflects the increasing trend toward laws requiring transparency in connection with all aspects of the use and disclosure of protected health information. New regulations specify that notification be made to impacted individuals no later than 60 days after the discovery of a breach, and notification must also be made to the Department of Health and Human Services. Beyond discharging notice obligations, a company should have an established and comprehensive process to manage security and privacy incidents in a timely and effective manner, to remediate privacy and security vulnerabilities, and to control the public relations challenges related to these incidents.

Assess business associates and related activities
Liability related to misuse or the inadvertent or inappropriate disclosure of protected health information does not stop at the border of the company’s group health plan. Rather, the group health plan continues to remain obligated for the actions of its business associates. Accordingly, a group health plan should undertake privacy and security assessments of those business associates that use and disclose protected health information on its behalf to enable the group health plan to secure protected health information in a manner no less secure than in its own environment.

Clearly, as HHS issues more guidance and companies establish more robust practices in response to increased requirements around HIPAA, companies and their group health plans should continue to reassess their controls and practices so they reflect and respond to current expectations, requirements, and industry practices. Notwithstanding the fact that changes will continue to emerge, companies should consider the foregoing actions as sound foundational activities.

Learn the latest on privacy without ever leaving your office.
Visit the IAPP’s online Educational Library.

FEATURED TITLE

Practical Privacy Series: Data Breach DVD
Get all six sessions from the 2007 IAPP Practical Privacy Series: Data Breach conference on DVD. Taped live at the event, this video offers a complete day’s worth of education on how to prevent, manage and recover from a data breach.

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

www.privacyassociation.org/edulibrary
Spying on staff  
continued from page 1

part of their efforts to root out corruption. In the case of the Deutsche Bahn, for example, the personal details—including names, addresses, and bank details of some 173,000 employees (including train conductors and others)—were compared with approximately 80,000 suppliers. In the case of Deutsche Telekom, officials tracked senior executives’ phone calls in order to identify the source in leaks of sensitive financial information to journalists.

Sanctions for unlawful spying on staff
In the wake of these privacy scandals, political leaders held an emergency summit in Berlin in February 2009. They agreed that an “Employee Privacy Act” should be included in an update of current data protection laws. This new law is expected to be accepted soon after the new German government is elected this fall. In the course of this legislative action, statutory provisions will be introduced which shall, inter alia, regulate if and under which conditions monitoring employees can be carried out lawfully.

Yet, even current applicable German data protection laws do not permit spying on employees in any case. Rather, many monitoring practices are unlawful and can be punished by harsh fines. Lidl experienced this quite dramatically. Its hidden-camera surveillance activities were found to have violated data protection laws and the company was ordered to pay a fine of 1.5 million Euros (approximately two million dollars). This is, by far, the highest fine ever issued by German data privacy watchdogs. Moreover, several managers from the companies caught up in privacy scandals have already lost their jobs, including the head of Lidl’s German operations, Frank-Michael Mros, and even Deutsche Bahn chief executive Hartmut Mehdorn—his justifications for the surveillance practices were found insufficient.

Therefore, in order to avoid such consequences, companies should ensure that all surveillance practices comply with legal requirements. Here they are in brief:

Data privacy background for employee surveillance measures
Even though, for the moment, Germany has no Employee Privacy Act, there are several laws that mandate rather strict protection of employee data. First of all, the provisions of the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) apply to the collection, processing, and use of employees’ personal data. Secondly, specific data protection obligations might follow from applicable Works Agreements.

Moreover, the employee’s privacy is protected by his or her respective personal right (allgemeines Persönlichkeitsrecht), which is enshrined in the German Constitution. In particular, the fundamental right on informational self-determination and the fundamental right on confidentiality and integrity of IT systems are significant constitutional guarantees for employment relationships in Germany. The employer is obliged to safeguard and promote the free development of its employees’ personalities (Sec. 75 (2) Works Constitution Act). On top of the aforementioned constitutional rights, labour courts’ extensive case law has developed principles for protecting the right to privacy of German employees.

Monitoring mechanisms in the workplace affect the privacy rights of employees. Under the BDSG, video surveillance of premises that are open to the public (which may include sale-rooms and restaurants) might be allowed, however, only subject to the following requirements: (1) there is no indication of a prevailing legitimate interest of the individuals and (2) the surveillance is necessary for the purpose of:

- enabling public agencies to fulfill their tasks;
- keeping out trespassers; or
- achieving justified interests in certain defined situations (e.g. suspicion of crime).

Employers must make clear in advance that surveillance will be conducted and must specify who will be included. The data must be deleted as soon as it is no longer needed for the defined purpose. Clandestine surveillance of public premises is not permissible at all.

More relevant in practice is the surveillance of premises with restricted access. According to case law, the right to informational self-determination of the employees implies that they can freely decide whether they may be videotaped and whether the
pictures can be used against them. Moreover, there is also protection for the spoken word. For example, the right to determine for oneself whether the spoken word should be available to the partner of the conversation only, or also made accessible to third parties or even the general public, and whether it may be recorded by electronic or other means.

The assertion of the overriding legitimate interests of the employer may justify interference in the employee’s privacy rights. When there is a conflict between the general privacy rights of the employee and the employers’ interests, the legally protected interests have to be weighed against the employers’ interests to determine on a case-by-case basis whether the general right to privacy merits priority.

According to the Federal Labour Court, clandestine surveillance by technical devices is only permitted if there is a:

- specific indication of a criminal offence or other serious misconduct at the expense of the employer;
- less drastic means to clear up the suspicion have been exhausted;
- covert surveillance is practically the only remaining means; and
- the surveillance is proportionate (for example, a cash deficit that cannot be cleared up in any other way).

Surveillance measures are not allowed to invade the employee’s private sphere. Therefore, video surveillance is never permitted in such places as changing rooms and toilets (which had reportedly happened at Lidl). Even if the employees have been informed that a video camera or a similar technical device will be installed at the workplace, it does not mean that surveillance is automatically admissible. In most cases, continuous surveillance is considered an infringement on employees’ personal rights due to the pressure brought about by the constant observation. This applies particularly in situations where the employer has the potential to use undetected surveillance. Again, in this case the interests of the employees have to be weighed against the legitimate interests of the employer.

The above-mentioned principles to safeguard the employee’s privacy also apply to other surveillance measures by employers, such as eavesdropping on employees’ phone calls. Employees must be notified in advance if such calls are to be intercepted.

Apart from this notification requirement, which is also enshrined in Article 10 of the EC Directive 95/46, the principle of necessity must be observed when monitoring employees. According to Article 6 para 1 (c) EC Directive 95/46, the data processing must be “adequate, relevant, and not excessive in relation to the purposes.” Privacy watchdogs have cast doubts as to whether the above-mentioned surveillance practices comply with these requirements. In particular, they have challenged that, for the purpose of fighting corruption, it is necessary to include every employee—indeed any employee—into the monitoring measures, irrespective of whether there had been a relevant risk for corruption in the individual case.

**Involvement of the Works Council and the data protection officers**

Additionally, the monitoring of employees triggers a co-determination right by the Works Council (sec. 87 para. 1 no. 6 of the German Works Constitution Act). The Works Council has a right of co-determination, especially in the event of the introduction and application of technical systems which are suitable for monitoring the conduct or performance of the employees. This will generally be the case for all surveillance systems, such as closed-circuit television (CCTV), and others.

Finally, in most of the cases mentioned above, the companies’ internal data protection officers had not been involved before the surveillance practices began, despite the data controller’s statutory obligation to inform the data privacy officer in good time of its plans for such data processing steps.

**Outlook**

It remains to be seen whether the legislator, when drafting the new Employee Privacy Act, will confine itself to merely taking over these existing restrictions on employee surveillance into the new law, or rather tighten the legal framework (as he currently plans to do for the marketing use of customer data). The Federal Ministry of Labour and Social Affairs, which will present the draft, has announced that it will not only attempt to regulate video surveillance but also will craft detailed provisions for issues such as e-mail and Internet monitoring in the workplace, and for protecting whistleblowers. The first announcements of ministry officials argue for a stricter approach. The declared aim of the new law is to specify the existing workplace rules, and to adapt them to the requirements of a modern working environment. Even more reason for companies to revise duly their employee surveillance and data governance practices in Germany.

**Flemming Moos** is an attorney at DLA Piper and chair of the IAPP KnowledgeNet in Hamburg, Germany. He is a certified specialist for information technology law and a member of the IAPP Publications Advisory Board. He can be reached at flemming.moos@dlapiper.com.
Social networking in the workplace

The ubiquitous presence and use of social networking sites (SNS) such as MySpace, Facebook, LinkedIn, and Twitter continues to shape how information is shared online among individuals. While the advent of SNS was generally within the context of personal communications, the use of SNS within the workplace raises privacy concerns for both employees and employers. Many employers permit employees some (limited) access to SNS for personal reasons, while other organizations have adopted SNS for official use within the organization internally or for external communications.

In May 2009, the Office of the Privacy Commissioner of Canada (OPC) issued a Fact Sheet “Privacy and Social Networking in the Workplace” to offer guidance on the use of SNS in the workplace.

The Fact Sheet notes that often, individuals, including employees who use SNS in the workplace, believe that personal SNS are private. The reality is that information posted on such sites can be accessed by many individuals for many purposes.

One of the OPC’s key recommendations is for organizations to create a policy on the use of SNS. The policy should specify:

• whether the use of SNS is permitted in the workplace;
• in what context and for what purposes SNS may be used;
• employer monitoring of SNS usage;
• whether SNS use is covered by any other rules;
• any other electronic network policies in place; and
• consequences for failure to comply.

The OPC suggests the policies include details on any company monitoring efforts, including off-duty monitoring, and reminds employers that certain monitoring could be considered a collection of personal information, therefore subject to privacy legislation in some jurisdictions.

SNS pose risks to organizations—from the inadvertent improper disclosure of confidential business information to deliberate sabotage by a disgruntled employee. Employees should remember that some personal and corporate information should be kept confidential, such as information about themselves, their co-workers, clients, and the organization. Failure to show a high level of discretion could result in the organization being held liable for such consequences as human rights complaints, copyright/trademark infringements, harassment charges, or other situations that could negatively impact the organization’s reputation and business interests.

Find the OPC Fact Sheet at www.privcom.gc.ca.

“Employees should remember that some personal and corporate information should be kept confidential…”

FRANCE

By Pascale Gelly and Elisabeth Quillatre

CNIL annual report 2008

The French data protection authority (CNIL) issued its 29th annual report on May 13. The 2008 report outlines the key topics addressed by the authority last year, such as peer-to-peer, video surveillance, processing activities around fraud, the G29 presidency, and more. The CNIL also presented data protection challenges, wondering whether privacy is an endangered sphere; how to best protect and
assist businesses, considering whether there should be no limit to European and international police cooperation, and whether surveillance of vulnerable people is justified. The authority also stressed its role in assisting businesses facing e-discovery requests.

The CNIL increased its staff resources to 120 last year and hopes for 132 staff members by the end of 2009. In 2009, the authority wants to work on its financing sources, and is very much in favor of having businesses that process personal data contribute to its funding.

The authority received 4,244 claims and completed 218 investigations in 2008, a 33 percent increase over the previous year. Twenty-five percent of investigations resulted from individuals’ claims. The CNIL issued 126 injunction letters to infringers. Most infringements have been resolved since only 10 entities were sanctioned (from mere warnings, to up to 30,000-Euro fines).

The report states that onsite investigations will remain a priority in 2009.

In addition, 3,679 organizations have appointed data protection officials (correspondants à la protection des données personnelles) leading to a total number of 989 DPOs, some being shared resources.

**Intelligent advertising screens under CNIL’s authority**

The CNIL conducted an onsite investigation of “intelligent” advertising LCD screens managed by the RATP (Paris public transportation company) and installed in one of the most frequented Paris subway stations at the beginning of this year. (See April 2009 Privacy Advisor, Global Privacy Dispatches, “Behavioral video surveillance in the Paris subway.”)

These “intelligent” devices broadcast ads and measure audience reaction via closed-circuit television (CCTV) cameras, enabling them to count the number of people stopping by and to calculate the time people spend looking at the ads.

During its investigation, the CNIL found that only statistical data were processed, and that images were neither recorded nor transferred to third parties, nor seen by providers.

Yet, the CNIL believes that this activity could be considered as processing of personal data, therefore subject to data protection law. The mere fact that statistics are issued after analyzing images of citizens’ identifiable faces, which are considered personal data under the European Directive 95-46-EC, supports this.

Thus, the CNIL considers itself competent to assess the legitimacy of these audience-measurement devices, as well as to assess the relevance of the data collected and to ensure that the rights of data subjects are guaranteed.

**Data transfer: a faster authorization process will come**

The law “simplification and clarification of the law; simplification of procedures” has finally been passed.

Previously, the CNIL individually examined requests for transfer authorizations during plenary sessions and authorized them by an express deliberation.

With this new law, the CNIL now gives its president the authority to authorize data transfers outside the European Union. The CNIL hopes this fast-track process will be used for routine types of data transfers.

Additionally, this new law lets the CNIL publish its opinion on bills at the request of the president of one of the Parliament’s permanent committees. It also simplifies the CNIL process to deliver a quality label for products and procedures intended to protect individuals’ privacy.

For more on this law, see the Privacy Advisor, March 2009, Global Privacy Dispatch article “Hope for a fast(er) data transfer authorization process.”

**Online store sanctioned for spam**

CDiscount, one of Europe’s most successful online discount retailers, has been sanctioned by the CNIL for non-compliance with a data subject’s right to object to the use of personal data for direct marketing purposes.

According to Article 38 of the French Data Protection Act, any natural person “is entitled to object, at no cost to himself, to the use of the data relating to him for purposes of canvassing, in particular for commercial ends, by the controller of a current or a further data processing.”

After failed attempts to unsubscribe from CDiscount mailing lists using the opt-out means provided by this data controller, several Internet users filed complaints with the CNIL. CDiscount claimed that technical problems with its software module were to blame, and that those problems had been resolved. Yet the CNIL continued receiving claims from Internet users who tried unsubscribing not only by clicking on the link, but also by e-mail, postal mail, and via a surcharged phone number, in vain. The CNIL then sent a formal notice to CDiscount. The notice went unanswered. The company said it was not delivered to the appropriate person in the company.

As a consequence, the CNIL imposed a €30,000 fine, stating that the Internet users’ requests were unfulfilled.

The CNIL acknowledged CDiscount’s commitment to appointing a data protection correspondent.

**HADOPI**

A High Authority for the distribution of works and the protection of rights on the Internet was created by the so-called HADOPI law, passed by the Senate on May 13.

See, Global Privacy Dispatches, page 12
Global Privacy Dispatches
continued from page 11

One of its missions is to protect copyrighted works from infringement committed over electronic communications networks.

It is entitled by law to obtain the data retained and processed by operators, as well as the identity and contact details of subscribers whose network access has been used to reproduce or provide protected works without authorization.

In case of infringement, the subscriber may receive a warning letter through the ISP. In case of a repeat infringement within six months, the commission may send a second recommendation. If another infringement takes place within the year following the last letter, then after contradictory proceedings, the commission may request the suspension of the network access (two months to a year) or issue an official injunction to prevent repeated infringements, unless a settlement is found with the subscriber.

Secondary legislation is necessary before this HADOPI law can be implemented in order to address, in particular, the means of appeal and the specificities of the data processing the High Authority may carry out.

This HADOPI law has given rise to controversies. Therefore, it is no surprise that this test is now challenged before the constitutional court.

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

Israel

By Dan Or-Hof, CIPP

Data breaches in government agencies
The State Comptroller and Ombudsman

“\The report reveals considerable flaws in the handling of highly sensitive information stored in these databases.\”

released an extensive report on the adequacy of privacy protection and information security in databases held and managed by the Ministry of Interior Affairs and the National Social Security Agency.

The report reveals considerable flaws in the handling of highly sensitive information stored in these databases. Among the findings: absence of information security supervisors required under Israeli law; absence of necessary procedures and logs of use; unlawful distribution of records over the public Internet; and harmful outsourcing procedures.

The National Social Security Agency’s head of information security informed the State Comptroller that the agency’s activities include severe breaches of privacy. However, the report did not prevent the agency from offering a new bill that would allow them to receive sensitive information from private companies, such as insurance companies and banks, as well as other governmental agencies, such as the State Tax Agency.

During an IAPP KnowledgeNet meeting in Tel Aviv, Mr. Yoram Hacohen, head of ILITA (the Israeli Law Information and Technology Agency) described the Ombudsman’s findings as an issue that should be addressed, and said that an investigation is underway.

Read more about the Tel Aviv KnowledgeNet event on page 19.

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.

The Netherlands

By Richard van Staden ten Brink

Dutch Senate blocks mandatory meters
On April 7, the Dutch Senate blocked a Dutch Minister of Economic Affairs proposal that would require Dutch consumers to install so-called “smart meters” in their homes.

Smart meters are digital electricity and gas meters that report real-time data on a household’s energy use to utility providers. Smart meters are supposed to help conserve energy because they enable improved management of energy networks (“smart grids”), and allow consumers to monitor their energy use on the Internet.

However, various senators contended that personal information collected and transmitted by smart meters could be intercepted by hackers and used for unlawful purposes. There was also concern that a requirement to install smart meters would violate Article 8 of the European Convention on Human Rights, the article that prohibits state interference with personal and family life that is not “necessary in a democratic society.”

After several days of debate, it became evident that the majority of the Senate was not ready to accept the proposal. The Minister decided to amend the proposal to allow consumers to choose between traditional or “smart” energy meters. However, this amendment will have to be accepted by Parliament before the Senate can consider it.

Richard van Staden ten Brink is advocaat at De Brauw Blackstone Westbroek in Amsterdam. He may be reached at richard@vanstadentenbrink.com.
Planning a summer vacation? Be a privacy-smart traveler

Many people are scaling back their summer vacation plans because of the current economic situation. Some are staying closer to home. Others may be taking shorter vacations. But it’s important to remember that when you travel, your risk of exposure to fraud and identity theft may increase. It’s a fact that people tend to let down their guard while on vacation. Criminals know this.

Identity theft is often a crime of opportunity. Don’t be a vacationer who presents a crook with that opportunity. Your personal information, credit and debit cards, driver’s license, passport, and other personal information are the fraudster’s target. A few minutes spent planning before you travel can help reduce the risk that a fraudster will ruin your vacation. Here are some tips to help you avoid any nasty surprises:

• Clean out your wallet. Remove unnecessary credit cards, your Social Security card, and other unneeded documents that could compromise your identity if lost or stolen while on vacation. If you have a Medicare card, make a photocopy without the last 4 digits of your Social Security number.

• Contrary to some advice, it’s best to carry two credit cards. Carrying too many credit cards will subject you to additional aggravation if your wallet is lost or stolen. But there’s a risk in carrying only one credit card if, for example, your card inadvertently becomes inactivated due to suspected fraud or if the magnetic strip becomes damaged. Having this happen while away from home could become a major headache.

• Photocopy or make a list of the remaining contents of your wallet. Keep it in a secure and locked location or with a trusted individual at home whom you can contact in case your wallet is lost or stolen.

• Do not leave your wallet or any documents containing personal information in your hotel room unattended. Hotel rooms are not the most secure places. Many people have access to the room. Use a hotel safe when available.

• Use traveler’s checks or credit cards for payment. Leave your checkbook in a secure locked place at home.

• Call your bank and credit card companies to let them know when and where you will be traveling. Their fraud departments may then monitor your accounts for unauthorized transactions during this time.

• Do not use or carry any debit cards (check cards). This reduces your vulnerability to having your checking account emptied while you are on vacation. See www.privacyrights.org/fs/fs32-paperplastic.htm#2 for an explanation of why debit cards are a very bad choice for consumers.

• If you plan on using an ATM card during your vacation, use one that does not have debit or check card privileges (one that always requires a PIN and does not contain a Visa or MasterCard logo). You can ask your bank to change an ATM/debit card to one that is “ATM only.” It’s best to use ATM machines found at banks or credit unions that are in well-lit areas. Be sure to examine the ATM machine carefully for signs of tampering. Be on the lookout for anything that looks suspicious.

• When dining in a restaurant, try to keep an eye on your credit card when you pay your bill. If the server removes your card from sight, they may be able to create a “clone” by using a portable card skimmer that will copy the information from the card’s magnetic strip.

• Ask your Post Office or a trusted neighbor to hold your mail for you. Mail that is left in an unlocked mailbox is a goldmine for identity thieves. It also sends a signal to potential burglars that your house is vacant.

• If you are bringing your laptop with you, be very careful when using it to access online banking or other password-protected services from Wi-Fi networks. Be sure to use Wi-Fi

Pause before packing PII

The lazy days of summer are just around the corner and the Privacy Rights Clearinghouse (PRC) has some advice for vacationers: don’t be lazy about your personal information. The PRC recently released tips for protecting PII while on summer holiday. A few minutes of planning, they say, can help prevent a ruined vacation. (Tips printed here with the permission of the Privacy Rights Clearinghouse, www.privacyrights.org.)
hotspots that are secure. For some Wi-Fi tips from the FBI, see www.fbi.gov/page2/may08/wifi_050608.html.

- If you are using cyber-cafés, hotel business centers, or other public-access Internet facilities, be aware that keyloggers (software that can track your keystrokes) may be tracking you. Public-access facilities may use servers that aren’t encrypted. Therefore, never access any sensitive information from a public computer.

- Always be cautious with the information you share on social networking sites. You wouldn’t put a sign on your front door saying “Away on Vacation.” When you broadcast your travel plans on a social networking site, you are doing the same thing electronically. This information can then be used by criminals who will know that you will be away from home.

If the worst should happen and you become a victim of identity theft, be sure to read Privacy Rights Clearinghouse’s Fact Sheet “Identity Theft: What to Do if it Happens to You” at www.privacyrights.org/fs/fs17a.htm.

Keith

You and some of your privacy peers are headed to a remote island where you’ll compete for the position of chief privacy officer. You can take only three privacy books with you. What are they?

I’d only need one: R.I.P.: Remote Island Privacy — The Essential Guide (publication pending)

What book most shaped your views on privacy?
Simulations, by Jean Baudrillard

What is the one privacy book you think everyone should read?
Landscaping for Privacy (Gardening & Landscaping), Sunset Books

What are you reading now?
Mind Manipulation: Ancient and Modern Ninja Techniques, by Haha Lung

What do industry experts consider to be best practices in preparing for and responding to a data breach?

BreachCenter.com is a dynamic content community for breach response professionals to collaborate on defining the issues, suggest a consensus view, and point corporations toward the path of effective breach response.

BreachCenter.com
INTERSECTIONS BUSINESS SERVICES

Powered by a leading provider of consumer and corporate identity risk management services. Please call us at 888-283-1725.
The dramatic rise of online social networking has elevated concerns about Internet child safety. There have been many technological, educational, and law enforcement efforts directed toward Internet safety, but privacy pitfalls can exist.

In this month’s edition of the Privacy Tracker newsletter, Braden Cox of NetChoice addresses the sensitive issue of Internet child safety, and how seemingly straightforward solutions to safety concerns can raise a host of privacy and social issues.

If you don’t yet receive the Privacy Tracker, subscribe today to access this article, monthly newsletters, a monthly call featuring expert analysis on pending legislation, and weekly updates on privacy legislation.

www.privacytracker.org
From Orange County to Barcelona privacy pros worldwide came together on June 25 to meet, talk and, in some cases, tweet privacy at Privacy After Hours events.

In Boston, IAPP members and friends twittered al fresco in a soft summer breeze. From left: Peter McLaughlin, CIPP, Foley & Lardner LLP; Tracey Hulme, CIPP; Colette Phillips, CPC Global; Agnes Bundy Scanlan, CIPP, Goodwin Procter LLP; Mary Helen Gillespie, CIPP; Rochelle Seltzer, Seltzer Design; Diane Ripstein, Diane Ripstein Consulting; George C. Bremner, CIPP.

Orange County, CA

All CIPPs. From left: Diane Charvat, CIPP, Experian; Eric Nelson, CIPP, Secure Privacy Solutions; Astra Bester, CIPP, Experian; Steve Wede, CIPP, Privacy Solutions.
Wellington, NZ

Wellington’s privacy pros waded through the issues well before the rest of us.

Washington, DC

More than a dozen came out for Privacy After Hours in Washington, DC.

Barcelona, Spain

Lawyers, luminaries, and technologists were counted among those at the Privacy After Hours in Barcelona, where “high caliber” conversation dominated the evening, according to hosts.

Cleveland, OH

Hitting privacy out of the park in Cleveland.

Dallas, TX

Privacy commanded attention at Privacy After Hours in Dallas.
Inspired Learning

The IAPP
Privacy Academy 2009
September 16 - 18
Boston Marriott Copley Place

REGISTER NOW
www.privacyacademy.org
The Israeli IAPP chapter conducted its third KnowledgeNet meeting on May 13. The meeting explored the conflict between the need to disclose personal information under U.S. e-discovery rules and European and Israeli data protection and privacy laws.

Mr. Steven Bennet, a partner at Jones Day in New York, talked about the U.S. law’s point of view and provided a comparative analysis of other countries’ laws. Mr. Bennet described the difficulties of producing personal information from other jurisdictions due to trans-border data flow limitations and discovery-blocking laws. Consequently, multinational companies are potentially subject to U.S. courts’ sanctions, and to presumptions that information not produced as required is harmful for the party that did not produce it.

The lecture portion addressed some solutions to the conflicting obligations, including EU Article 29 Data Protection Working Party suggestions to anonymize information and to process the information locally. A Sedona Conference whitepaper on proposed methods for handling the jurisdictional conflicts related to e-discovery provided further reference on this issue.

Mr. Bennet also mentioned a party’s ability to refuse discovery on grounds that the information is not reasonably accessible or causes an undue burden or cost. Mr. Bennet concluded that, evidently there is no magic solution. Dr. Omer Tene, co-chair of the IAPP’s Israeli KnowledgeNet chapter, described the challenges that Israeli companies face in that regard. Dr. Tene discussed the need for companies to form adequate document immigration policies, the feasibility of anonymizing information, and the option of utilizing protective and confidentiality orders to limit the scope of data disclosure.

E-discovery and privacy

By Dan Or-Hof, CIPP

The Israeli IAPP chapter conducted its third KnowledgeNet meeting on May 13. The meeting explored the conflict between the need to disclose personal information under U.S. e-discovery rules and European and Israeli data protection and privacy laws.

Mr. Steven Bennet, a partner at Jones Day in New York, talked about the U.S. law’s point of view and provided a comparative analysis of other countries’ laws. Mr. Bennet described the difficulties of producing personal information from other jurisdictions due to trans-border data flow limitations and discovery-blocking laws. Consequently, multinational companies are potentially subject to U.S. courts’ sanctions, and to presumptions that information not produced as required is harmful for the party that did not produce it.

The lecture portion addressed some solutions to the conflicting obligations, including EU Article 29 Data Protection Working Party suggestions to anonymize information and to process the information locally. A Sedona Conference whitepaper on proposed methods for handling the jurisdictional conflicts related to e-discovery provided further reference on this issue.

Mr. Bennet also mentioned a party’s ability to refuse discovery on grounds that the information is not reasonably accessible or causes an undue burden or cost. Mr. Bennet concluded that, evidently there is no magic solution. Dr. Omer Tene, co-chair of the IAPP’s Israeli KnowledgeNet chapter, described the challenges that Israeli companies face in that regard. Dr. Tene discussed the need for companies to form adequate document immigration policies, the feasibility of anonymizing information, and the option of utilizing protective and confidentiality orders to limit the scope of data disclosure.
EXPLOITING PASSWORD POWERS
A study of 400 senior IT professionals in Britain and the United States revealed that 35 percent abuse administrative passwords to access confidential data. The top area of interest to the snoopers was human resources records, followed by customer databases and merger plans.

Source: Reuters

CHECKING E-MAIL
Known as the “Nokia Act,” an amendment to Finland’s Protection Law on Electronic Communications passed into law in March. It gives employers the right to access certain employee e-mail information and attachments in an effort to prevent confidential company data leaks. Prior to the amendment, only police had access to such information.

Source: IT News

VIEWING PROFILES
While most business executives believe they are entitled to know about their employees’ social networking activities, most employees say butt out. That’s according to the results of a Deloitte survey of 2,000 U.S. adults. Of the 500 management-level respondents, 60 percent felt they had a right to know, while 53 percent of employee respondents said information they post to social networking sites is none of their employer’s business.

Source: Wall Street Journal

Encryption gets “Gentry”-fied

IBM researcher Craig Gentry discusses breakthrough

Last month, IBM announced that researcher Craig Gentry made a cryptographic breakthrough with big implications for data privacy. The so-called “fully homomorphic encryption” technology is years away, according to IBM, but its promise for companies that handle and store individuals’ data is anticipated to be profound.

“[Fully homomorphic encryption] would give us new confidence that you can secure the world’s infrastructure and bring intelligence to it without exposing data to greater risks,” the head of IBM’s research arm told Forbes.

Researcher Craig Gentry discusses the breakthrough here.

IAPP: Is the anticipated implementation platform-neutral (i.e., will it support any database structure)?

Gentry: Yes. Abstractly, you can view a ciphertext as a secure box that holds a message. Now, suppose that you have several messages m_1, ...m_t (or several database entries) that are encrypted under the same public key—i.e., the messages are, in some sense, inside the same box. If the encryption scheme is fully homomorphic, then, for any efficiently computable function f, you can use the encryptions of m_1, ..., m_t to compute a ciphertext that encrypts f(m_1, ..., m_t) — i.e., you get f (m_1, ..., m_t) inside the same box—and you can compute this new ciphertext without the secret decryption key.

For example, a user could store encryptions of m_1, ..., m_t on a database server. Suppose that the user later wants some function of its data—i.e., f(m_1, ..., m_t). This function f might be a JOIN query, or it might output all of the entries containing some substring, ... whatever. Using the fully homomorphic encryption scheme, the server can compute an encryption of f(m_1, ..., m_t), send that ciphertext to the user, and the user decrypts it to recover the desired information.

Again, as long as you can compute the function f reasonably efficiently, then you can compute the same function over encrypted data (getting an encrypted result), though computing the function over encrypted data takes much longer. In particular, the scheme is independent of the data structures used. (In contrast, most likely the function f that you want to compute would be dependent on the data structure.)

IAPP: Does the current implementation encrypt at the table, column, or field level, or are these reference models inapplicable?

Gentry: There isn’t an “implementation” yet; currently, there is only a mathematical description of the scheme.

The reference models are inapplicable, as stated above. Any program or database-querying system could be “compiled” into an (encrypted) program or (encrypted) system that has encrypted input and output.

IAPP: How does it compare to other fully homomorphic encryption schemes? What makes it different?

Gentry: There aren’t any other fully homomorphic encryption schemes. A bit more accurately, and to get a bit technical, there are previous schemes but their performance (running time) depends *exponentially* on the function f that you are computing, whereas the running time of my scheme depends...
only *polynomially* on the function f. In other words, to put it simply, even though my current scheme is rather slow, previous schemes would be much, much slower—ridiculously slower—for mildly complex functions f.

**IAPP:** A Forbes article on your scheme mentioned that the current application is cumbersome, and that years of newly developed efficiencies will be required to make it commercially viable. Can the technology be implemented (albeit, inefficiently) on typical current datawarehouse hardware, or are you anticipating that hardware advances over the coming years would make this viable? Is the sense that optimization of the algorithm will improve performance, or that computing hardware will advance to make this unnecessary?

**Gentry:** I’m optimistic that, over the next couple of years or so, researchers will find ways to make the algorithms themselves significantly faster, and that the algorithmic speed-up will be much larger than the hardware speed-up over this period. I think it makes sense to find this low-hanging fruit before commercializing it.

It’s dangerous to speculate on when it will be ready to be used on databases...

One issue is that, although part of the appeal of my scheme is that it is “fully” homomorphic in the sense that it can handle arbitrary functions f, my scheme performs significantly better if the complexity of the function f falls below a certain threshold. Once the complexity of f goes above a certain threshold, I need to use a technique that I call “bootstrapping,” a computationally-intensive operation in which I “refresh” the intermediate ciphertexts on my way to computing the eventual output ciphertext (an encryption of f(m_1, ..., m_t)). However, if the complexity of f falls below the threshold, I can get by without using bootstrapping, and the scheme is much closer to being practical for such functions. I would imagine that relatively simple functions, such as a JOIN operation in a database query, would fall into this below-the-threshold category.

---

**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 April & May 2009:

- Julian Appel, CIPP/C
- David Williams Badanes, CIPP
- Courtney Ingraffia Barton, CIPP
- Matthew Beckwith, CIPP
- Mary Katherine Bedek, CIPP/C
- Daisy Tracy Bennett, CIPP
- Gladys Bertrand, CIPP
- George C. Brenner, CIPP
- Eric Andrew Brothers, CIPP
- Thomas Averill Buchanan, CIPP
- Lu Cao, CIPP
- Katie Concoran, CIPP
- Daniel A. Curtis, CIPP
- Dean Mitchell Dolan, CIPP/C
- Carol E. Farer, CIPP/G
- Emma J. Fletcher, CIPP
- Scott Gramm Gagnon, CIPP/G
- Patricia E. Gant, CIPP
- Jasmine Gill, CIPP
- Ingrid Ringman Gliottone, CIPP
- John Edward Gunther, CIPP
- Patricia Guroff, CIPP/G
- Kyle Joseph Harvey, CIPP
- Frances Jane Henderson, CIPP
- Andrew L. Hoffman, CIPP
- Christal L. Hoo, CIPP/G
- Jenny Lee Hoots, CIPP/G
- Andrea Renae Husted, CIPP/G
- Rose Iannone, CIPP/G
- Paul Gregory Krieger, CIPP
- Paul Roman Lazarr, CIPP
- Mark William Littlefield, CIPP/G
- John J. Liut, CIPP/C
- Bruce Lowe, CIPP/C
- Brian Jeffrey Masch, CIPP
- Meaghan Kathleen McCloskey, CIPP
- Brian McDonald, CIPP
- Camille Antoine Quo, CIPP
- Vickie S. Miller, CIPP
- Karen Ann Milliet, CIPP
- Michael Frederick Muhleisen, CIPP/G
- Carolyn S. Munoz, CIPP
- Joanna Chi-Wei Murphy, CIPP/C
- Gurappa Padasali, CIPP
- Shirley Padgett, CIPP/G
- Michael Gus Pallas, CIPP
- Dyan Jo Palmer, CIPP
- Vickie Papapetrou, CIPP
- Joseph Samuel Pecora, Jr., CIPP
- Tim Penrose, CIPP
- Guillermo Perez, CIPP
- Denise Ragland, CIPP
- Rachel Ann Ralston, CIPP
- Cheryl M. Rogovin, CIPP
- Richard J. Ryan, CIPP
- Ahmad M. Sabbarini, CIPP
- Jennifer Lynne Sebeck, CIPP
- Amber Amaretta Smith, CIPP/G
- Leah Michele Smith, CIPP/C
- Gina Marie Spada, CIPP
- Kevin W. Stout, CIPP/G
- Michael Jason Stull, CIPP
- Heather Egan Sussman, CIPP
- Kristie A. Swanson, CIPP
- Rita H. Vale, CIPP
- Jane Marie Van Alphen, CIPP/C
- Judith L. Vars, CIPP
- Jane Marie Van Alphen, CIPP/C
- David A. Wainberg, CIPP
- Hugh Oliver Wentz, Jr., CIPP
- Sam Ashford Welch, CIPP/G
- Cathy Ann Wichert, CIPP
- Thomas Witwicki, CIPP
- Adam S. Wright, CIPP
- James Young, CIPP

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

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


Even better, an employer should arrange for copies of all messages to be stored on the employer’s own systems. These copies are very useful as backups, and for litigation purposes. Moreover, copies stored on the employer’s equipment are not subject to the Stored Communications Act, and may be reviewed by the employer without an employee’s prior notice or consent. See Hilderman v. Enea, 551 F. Supp. 2d 1183 (S. D. Cal. 2008).

All employers should have a policy on the use of its electronic resources and communications systems, and should have employees acknowledge the policy or agree to its terms. Such a policy should make clear that all systems and messages are the property of the company; that employees should use them for business purposes only; that they should have no expectation of privacy with respect to their use of the systems or the messages they send; that the employer can and will review employee messages; that the employee agrees that any vendor of messaging services may provide copies of all messages to the employer; misuse of the systems is prohibited and may result in termination of employment; and that the policy may not be modified orally, but only in writing by a company officer.

For more on the topic of employee monitoring, see the article “Employee monitoring technologies and data privacy—no one-size-fits-all globally” in the May issue of the Privacy Advisor.

Brian O’Connor, CIPP, is chief security and privacy officer at the Eastman Kodak Company, where he coordinates the development and implementation of employee data and information security policies. He directs Kodak’s Corporate Security group, which conducts investigations, manages a global badge and access control system, and provides executive protection services. Before his appointment as CSPO, O’Connor was senior counsel in Kodak’s Employment Law Legal Staff, advising management and human resource professionals on all legal issues relating to applicants, employees, and former employees.

Amy Yates, CIPP, is a director in the Security and Privacy Services practice at Deloitte & Touche LLP, and is aligned with its Security and Privacy Services Center of Excellence. She advises domestic and international clients on a wide range of privacy and data protection issues, working with clients to develop business solutions for addressing complex data protection requirements. Before Deloitte, Yates served as the chief privacy officer for Hewitt Associates LLC, where she established and led Hewitt’s Privacy Office and its global privacy program for five and a half years.

NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION

FUNNY NAME... SERIOUS BUSINESS...

We get a lot of ribbing and puzzled looks when people hear our name. But thankfully, most privacy and information security professionals take us very seriously.

Improperly discarded paper and electronic records are among the most overlooked and vulnerable areas of information protection. Information destruction has also become an area of increasing regulation, enforcement actions and fines.

Since 1994, the National Association for Information Destruction (NAID) has been the leading proponent of standards development and education related to proper information disposal.

NAID’s 1,000-plus service providers around the world are dedicated to helping organizations make informed decisions on records destruction, vendor selection, employee training, contract language and policy development.

Get serious about information disposal - www.naidonline.org
Privacy in Print
Perusing recently released privacy publications

Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society

By Ian Kerr, Valerie Steeves, and Carole Lücock, 2009, Oxford University Press.

On the identity trail

By David Morgan, CIPP, CIPP/C; Debra Farber, CIPP, CIPP/G; and Julie Sinor, CIPP

Ian Kerr, Valerie Steeves, and Carole Lücock of the University of Ottawa have recently released Lessons from the Identity Trail, one of four volumes produced by On the Identity Trail, a major interdisciplinary research initiative lead by Professor Kerr. Of interest to both academics and privacy professionals, the book is organized into 28 chapters, each consisting of a paper representing a distinct view on the topics of anonymity, privacy, and identity in our rapidly-evolving, highly-networked society.

With such a diverse set of disciplines represented, Lessons from the Identity Trail is guaranteed to expose you to a new perspective or way of thinking. From the opening chapter on surveillance and consent—in which we learn about temporal effects on perceived privacy benefits and losses—the sections on privacy and anonymity introduce a host of interesting theories: that privacy can be improved in digital social environments using heuristic evaluation of protections, that privacy empowers battered women instead of oppressing them, that future participation in society might depend on holding an ID card, and that pop music stands to raise public awareness of surveillance more effectively than the written word can. In the final section, anonymity is considered in a legal context in North America and Europe.

For more about the On the Identity Trail project, or to download the free version of Lessons from the Identity Trail, visit www.idtrail.org.

David Morgan, Debra Farber, and Julie Sinor are members of the IAPP Publications Advisory Board.

Their Information
Your Reputation
Our Experience.

Affinion Security Center’s BreachShield™ offers data breach protection services that empower companies to provide quick, superior and compliant safeguards.

Be Prepared. www.breachshield.com

For more information on the Affinion Security Center please visit www.affinionsecuritycenter.com.
IN MEMORIAM

The field of data privacy lost a dear friend recently. After a brief struggle with pancreatic cancer, Mike Hubbard passed away on Sunday, June 28.

Mike’s long contributions to the privacy profession belie his too-short life. He was very active in the IAPP healthcare-pharma working group for many years, sharing his expertise as a top healthcare privacy attorney, HIPAA expert, and prominent member of the North Carolina privacy bar. He became United Healthcare’s chief privacy officer about a year ago.

Mike was devoted to his field. Even during the days that followed his diagnosis, privacy was top-of-mind. In documenting her husband’s illness, Mike’s wife tells the story about how, when she joined a blog devoted to those dealing with terminal illness, his first question was about the blog’s privacy policy.

Most of us last saw Mike at the IAPP Privacy Summit in March. He was struggling with the disease then, but few knew. To the last, his professionalism and his passion for privacy could not be doused.

The privacy field is better for Mike Hubbard.

Pascale

You and some of your privacy peers are headed to a remote island where you’ll compete for the position of chief privacy officer. You can take only three privacy books with you. What are they?

1. A book big enough to use as a screen to protect my privacy

2. The Information Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risk, by Margaret P. Eisenhauer

3. Binders of Article 29 Working party papers

What are you reading now?
The Blind Assassin, by Margaret Atwood
The Goodwin Procter - IAPP Privacy Vanguard Award

Who says “Vanguard” to you?

Who will it be next?

They are leaders and luminaries. They stay ahead-of-the-curve, always aiming for the highest standard (and usually attaining it). Their career achievements will leave a mark on the data privacy field forever. They are the Privacy Vanguard award winners.

The IAPP and Goodwin Procter will present this year’s award to the professional who best demonstrates outstanding leadership, knowledge, and creativity in privacy and data protection.

But they can’t do it without you.

Tell us who should receive the Vanguard award.

Submit your nomination by July 24 at www.privacyvanguard.org.

Then, join us at the 2009 Privacy Dinner in Boston for the award presentation!

Nuala O’Connor Kelly, CIPP/G
2006 Privacy Vanguard award winner

Harriet Pearson, CIPP
2007 Privacy Vanguard award winner

Marty Abrams
2008 Privacy Vanguard award winner

???
2009 Privacy Vanguard award winner

Also accepting nominations for Innovation Awards

Nominate an organization for the HP-IAPP Privacy Innovation Awards. The Innovation Awards recognize those public- or private-sector organizations that have demonstrated the year’s most effective integration of privacy programs or services.

Nomination deadline: July 24

Organizations from all industries and areas encouraged to apply.

For more information: www.privacyinnovation.org
Two University of Guelph students will use $50,000 from the Office of the Privacy Commissioner of Canada to further research on what motivates individuals’ disclosure of personal information on Facebook.

PhD candidates Amy Muise and Emily Christofides published research last year showing that a drive to be popular prompts university students to divulge personal details on the site. With the OPC funds, the researchers will expand the study to include high school and adult populations.

The grant was one of 11 awarded through the OPC Contributions Program, which helps advance critical research in the areas of privacy and data protection.

**My ID Score**

A new Web site helps you assess your identity fraud risk for free.

My ID Score runs basic, user-submitted information through a vast fraud database to discover transactions and potential fraudulent activities.

The site was created by identity fraud specialists ID Analytics, which uses its ID network to come up with a personalized score indicating how likely you are to becoming a victim of identity theft.

~ For more information visit www.privcom.gc.ca ~
CIRA review

The nonprofit organization that manages dot-ca domain names has launched consultations on the more privacy-sensitive disclosure policy it introduced last June. Over the next few months, the Canadian Internet Registration Authority (CIRA) will conduct one-on-one interviews and surveys and will host forums and open mic sessions to find out what members think of the new rules.

With some exceptions, the new policy prohibits the release of information on individuals associated with a domain name. Before the change, those searching could find individuals’ names and e-mail addresses.

“We wanted to revisit the issue to make sure we balanced the...desire for privacy and the desire for getting access to information where people have a legitimate need for it,” CIRA general counsel Michael Stewart told CBC News.

Visit www.cira.ca to participate or find out more.

Researchers wanted

The British Information Commissioner’s Office (ICO) is soliciting bids for a three-month research project aimed at putting a price tag on failures to protect privacy. The “business case for investing in proactive privacy protection” project will determine the cost of not having proper data protection safeguards in place, so organizations can “place a monetary value on information as an asset, quantify the risks of holding information, and pinpoint the financial and reputational costs should problems occur,” according to an ICO press release.

ICO Assistant Commissioner Jonathan Bamford said: “We are aware that one of the barriers to more proactive privacy protection within organizations is the absence of a soundly argued business case for expenditure. However, organizations can no longer afford to ignore data protection and CEOs need to wake up to the risks and responsibilities that come with vast data collection. Data protection needs to be taken as seriously as health and safety by those at the top of the corporate structure.”

Let’s collaborate

Privacy leaders ranked how important it is for their organization’s privacy function to collaborate with other corporate functions, revealing that:

- 100 percent feel collaboration with Information Security is very important or important;
- 98 percent feel collaboration with Information Technology is very important or important;
- 93 percent feel collaboration with Regulatory Compliance is very important or important;
- 83 percent feel collaboration with Human Resources is very important or important.

According to the results, important to a lesser extent is collaboration with:

- Corporate ethics;
- Physical security;
- Internal audit;
- Records management;
- Marketing;
- Government affairs; and
- Public relations and procurement.

Those who attend the IAPP Privacy Academy 2009 will receive the full findings of the Ponemon Institute-International Association of Privacy Professionals benchmarking survey at no cost.

Register at www.privacyacademy.org

Breaching data

Seventy percent of UK enterprise and public-sector organizations polled for a Ponemon Institute study have experienced at least one data breach incident within the last year. That’s an increase of 60 percent from the previous year.

Source: Ponemon Institute
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

Calendar of Events

**JULY**

15-17 Symposium on Usable Privacy and Security (SOUPS) Google Mountain View, CA
http://cups.cs.cmu.edu/soups/

16 IAPP Audio Conference – The Evolving World of “Reasonable” Security
www.privacyassociation.org/audioconferences

24 Goodwin Procter-IAPP Privacy Vanguard Award Nominations Deadline
www.privacyassociation.org/

24 HP-IAPP Privacy Innovation Award Nominations Deadline
www.privacyassociation.org/

**AUGUST**

29 IAPP KnowledgeNet – San Francisco (Palo Alto Location)

**SEPTEMBER**

18 IAPP Certification Testing – Boston, MA
Certification Foundation, CIPP, CIPP/G and CIPP/C Exams

**NOVEMBER**

3 IAPP Data Protection and Privacy Workshop – Madrid, Spain
(Preceding the 31st annual International Conference of Data Protection and Privacy Commissioners, November 4-6)

**DECEMBER**

8 Practical Privacy Series: Government
Washington, DC

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