In January this year, news broke of a massive credit- and payment-card data theft from TK Maxx (the UK division of TJ Maxx). TJX, the parent company, said that the theft occurred in May 2006, but it did not discover this until December 2006. In an updated announcement in February, it said the theft might have occurred in July 2005, but in papers filed with the U.S. Securities and Exchange Commission in March, it clarified that 45.6 million credit and debit card numbers were stolen over 18 months.

This article examines some of the data privacy law implications of the data theft from the UK perspective, identifying key elements of the Data Protection Act of 1998 that are relevant.

**The Data Protection Act and the Processing of Personal Data**

The Data Protection Act regulates the processing of “personal data,” that is, information relating to identifiable living individuals. It is conventional to treat credit and payment card data as personal data and there is no doubt that the Data Protection Act applied to TK Maxx’s processing within the UK. As such, TK Maxx was, and is obliged, to comply with the “data protection principles.” In the context of this case, breaches, the report focuses on the following key elements of the identity theft problem:

- Prevention, through providing enhanced security for information that can lead to identity theft;
- Prevention, in terms of making it more difficult for identity thieves to mis-use or take advantage of personal information;
- Improving identity theft victim recovery activities; and
- Law enforcement efforts to investigate, prosecute and punish identity thieves.

This coordinated strategy creates an ongoing series of action steps for the federal government, its state and local law enforcement partners and all entities that create and maintain personal information. The plan describes a continuing effort to make identity theft harder to commit, harder to profit from and easier to investigate and prosecute.

By Stewart Room

In January this year, news broke of a massive credit- and payment-card data theft from TK Maxx (the UK division of TJ Maxx). TJX, the parent company, said that the theft occurred in May 2006, but it did not discover this until December 2006. In an updated announcement in February, it said the theft might have occurred in July 2005, but in papers filed with the U.S. Securities and Exchange Commission in March, it clarified that 45.6 million credit and debit card numbers were stolen over 18 months.

By Kirk J. Nahra, CIPP

On April 23, 2007, the President's Identity Theft Task Force, led by the Attorney General and the Chair of the Federal Trade Commission (FTC), released a report that describes a coordinated strategic plan to reduce injuries from identity theft and take more aggressive action against identity thieves.

This report contains extremely useful information for companies and individuals interested in the ongoing fight against identify theft. In particular, aside from the vast array of useful detail about security practices, current privacy/security statutes and recent data breaches, the report focuses on the following key elements of the identity theft problem:

- Prevention, through providing enhanced security for information that can lead to identity theft;
- Prevention, in terms of making it more difficult for identity thieves to mis-use or take advantage of personal information;
- Improving identity theft victim recovery activities; and
- Law enforcement efforts to investigate, prosecute and punish identity thieves.

This coordinated strategy creates an ongoing series of action steps for the federal government, its state and local law enforcement partners and all entities that create and maintain personal information. The plan describes a continuing effort to make identity theft harder to commit, harder to profit from and easier to investigate and prosecute.

See, *ID Theft Task Force*, page 3

See, *TK Maxx Data Theft*, page 11

**This Month**

- J. Trevor Hughes on Breach Planning and Prevention ..........Page 2
- Global Privacy Dispatches ...............Page 4
- IAPP in the News ..................Page 12
- New Faces at the IAPP ..........Page 13
- Q & A: Ask the Privacy Expert: ......Page 14
- Calendar of Events .................Page 16
- Certification Graduates .......... Page 18
- Privacy News ....................Page 18
- Privacy Classifieds ..........Page 19
- The Lighter Side of Privacy ........Page 19
Notes from the Executive Director

Prepare Now or Pay Later

In May, the list of security breaches continued to grow with new entries for lost and stolen laptops and tapes containing sensitive data. We also learned new details of the financial damage facing TJX Cos., a price tag that already has cost the company $25 million, with no end in sight. The legal fallout continues to take shape for TJX, which is faced with multiple class action lawsuits and investigations by regulators. It seems obvious that companies would have learned — either by the excruciating example of others or their own data security blunders — that breach prevention is a wise up-front investment.

Then late last month came the stunning results of research conducted by The Ponemon Institute on behalf of Scott & Scott, a law and technology services firm. The study, titled ”The Business Impact of Data Breaches,” found that about 85 percent of 700 C-level executives, managers and IT security officers said their companies had experienced a data breach — yet nearly half of those respondents said that they had no breach response plan.

The study convincingly offers up the case for preparedness with more data. About 75 percent of the respondents whose companies experienced a data breach indicated they lost customers. Sixty percent of the executives and managers said they were likely to face litigation. One-third reported the likelihood of fines, and 32 percent said their organizations suffered a decline in share value.

As privacy professionals, we owe it to our organizations to make sure they are prepared for the inevitable day when data loss is no longer something that happens to other organizations. While some CPOs may understand the importance of breach planning and prevention, they may not know exactly how to go about preparing their company to respond proactively and thoughtfully to quell the breach storm and minimize the damage to their organization and its reputation.

Recognizing the vital importance of this endeavor, the IAPP is aptly prepared to respond to this urgent need in the marketplace. This month, we are offering a Data Breach conference during the inaugural Practical Privacy Series, June 27-28, at the Graduate Center, The City University of New York. SAI Global is the Platinum sponsor of these new events, which also include a day-long conference devoted to Financial Services and a third conference focused on Pharma/Healthcare.

If you have yet to register for the Practical Privacy Series, we urge you to review the agenda at www.privacyassociation.org. See you in New York City!

J. Trevor Hughes, CIPP
Executive Director, IAPP

Attention IAPP Members: We’ve Moved!

As the IAPP continues to expand our offerings and staff to better serve you, we’ve relocated to a new office space to accommodate our growing organization. Please note our new address:

170 Cider Hill Road
York, Maine 03909

The IAPP’s phone number and email addresses will remain unchanged. Watch for more information coming soon.
Action Plan and Key Elements for Private Companies

Beyond the key elements of the report, it is critical for private entities — the companies that collect, maintain and disclose the personal information that can be misused to commit identity theft — to review the key elements of the report and to understand the major action items and implications contained in it. Here are some of the key topics for Corporate America stemming from this report:

• **Start a project related to SSNs**
  The Strategic Plan makes clear that the Social Security Number (SSN) is the single most sensitive piece of data, with the highest likelihood of identity theft risks. While there is an increasing variety of laws relating to the use, collection and disclosure of SSNs, these laws impose only modest formal restrictions on how they can be used and disclosed by private companies.

  Despite this limited legal environment, however, all private companies should institute a specific management project to understand — across the company — how the SSN is obtained, collected, stored and disclosed. It is clear — throughout Corporate America — that SSNs are collected, disclosed and maintained for purposes that are either unnecessary or inappropriate. Most companies have no firm idea of all the places in the company where an SSN may exist. Each of these SSN contact points creates a realistic risk in connection with identity theft. It is only through an organized effort — by each individual company — that appropriate steps can be taken to reduce access to SSNs and the related risks of inappropriate use and or disclosure.

• **Overall security practices**
  The report also emphasizes the importance of improving overall security practices, in both private industry and throughout the government. Companies in many industries face existing requirements to develop and implement appropriate security plans. Companies in all other industries should be aware of the B.J.’s Wholesale case, where the FTC imposed liability on a company for a failure to implement reasonable and appropriate security procedures, despite the absence of either a specific legal requirement or representations to customers about security practices. In addition, there is an increasing likelihood of formal federal legislation imposing broad security requirements across all industries.

  Whether motivated by specific legal requirements or not, all companies should understand the need to develop and implement appropriate security practices. These practices do not need to meet a “perfection” standard. Instead, the existing legal standard requires “reasonable and appropriate” security practices. But these obligations require an ongoing effort to develop security policies and to impose stricter security practices across all aspects of a company. A failure to create reasonable and appropriate security creates both practical risks of security breaches and an increasing array of legal and financial potential liabilities.

  In addition, the report highlights the need for an ongoing security program to stay abreast of both technological developments and new issues that become visible as security risks. The past year has featured a flood of cases involving stolen or lost laptops. Clearly, companies need to evaluate their use of laptops, including encryption programs and new practices related to the storage of information on laptops. Similarly, PDAs, Blackberries and other portable media create a new category of risks, often outside of the traditional security practices of companies. This need for re-evaluation of security practices is ongoing and crucial.

• **Be aware of “low tech” security risks as well**
  While companies must evaluate their security practices, they must recognize

*See, ID Theft Task Force, page 8*
Global Privacy Dispatches

Editor’s Note: This is the first installment of Global Privacy Dispatches, a new monthly feature in the Advisor. Writers interested in summarizing privacy and security news in their country or region may contact ann.donlan@privacyassociation.org.

CANADA
By Terry McQuay

Privacy Law Report Calls for Breach Notice Provision

The much-anticipated report of the Parliamentary Committee that conducted the statutory 5-year review of Canada’s privacy law — the Personal Information Protection and Electronic Documents Act (PIPEDA) — was tabled recently in the House of Commons.

The report calls for limited changes to PIPEDA at this time, making 25 recommendations, many of which aim for greater harmonization among the federal privacy law and the provinces of Quebec, Alberta and British Columbia, all of which have substantially similar private sector data protection laws.

Some of the Commons Committee on Access to Information, Privacy Ethics recommendations are:

- The act be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the privacy commissioner. The committee also recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a “without consent” power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

- The federal Privacy Commissioner should not be granted order-making powers at this time.

- No amendment be made to PIPEDA with respect to the privacy commissioner’s discretionary power to publicly name organizations in the public interest.

- A definition of “business contact information” be added to PIPEDA.

- PIPEDA be amended to clarify the form and adequacy of consent required by it, referring to the Alberta and B.C. acts to better distinguish between express, implied and deemed/opt-out consent.

- The federal government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amending PIPEDA in this regard.

- No amendments be made to PIPEDA with respect to the transborder flow of personal information.

The report will now be considered by the federal government for any further action.

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.

EU
By Steve Kenny

Member States face Sept. 15 Deadline to Comply with Data Retention Directive

The 2006/24/EC directive on the retention of data amends directive 2002/58/EC, and must be brought into place by all member states by Sept. 15, 2007. Due to national security concerns, the new directive obliges public telephony operators and Internet service providers to retain personal data, such as the calling number, the user ID, and the identity of a user of an IP address, for a period of 6 to 24 months. EU member states are expected to implement widely varying compliance requirements at or above the minimum compliance requirements of this directive.

Steve Kenny is Principal Advisor, Privacy Services Leader for KPMG, based in London. He may be reached at steve.kenny@KPMG.co.uk.

“The report calls for limited changes to PIPEDA at this time ....”
**FRANCE**

By Pascale Gelly

Short Privacy Notices? Not in France!

A new decree (25 March 2007) addresses the content and medium of privacy notices. Individuals must be provided with the contact details of the department in charge of receiving requests for access, objection and rectification.

In addition, in case of transfers outside the EU, the notice must list the countries to which data is transferred; the nature of the transferred data; the categories of recipients; the level of protection given by the importing countries; the references to the European Commission adequacy decision if the importing country is “adequate,” and if not, the references to the Commission Nationale de l’Informatique et des Libertés (CNIL) authorization; or the exception justifying the data transfer. In addition, the data privacy notice must be posted on the data collection document.

When data is collected remotely, the notice must be read to the concerned individuals who must be offered to receive a copy in writing. The requisite must be made available to an employee if they have been taken into consideration to make a decision about a raise, a promotion, an assignment, etc. “

Access by Employees to Performance Evaluation

Following complaints made against a multinational company, the CNIL recently has reminded that “…‘ranking’ and ‘potential’ are data elements which must be made available to an employee if they have been taken into consideration to make a decision about a raise, a promotion, an assignment, etc.”

**CNIL Fines Another Multinational Company**

After having sanctioned the Crédit Lyonnais last summer, the CNIL has issued its second-highest fine against the French affiliate of the group Tyco Healthcare. The company, after the receipt of an injunction notice by the CNIL to provide information relating to an HR database for the global management of careers, responded that it had suspended the processing of what the CNIL Secretary General characterizes as a “computerized monster.”

According to the CNIL, “An on-site investigation showed that not only the implementation of the database had not been suspended but it was used and updated regularly in spite of the numerous legal uncertainties raised by the CNIL (among others: purposes, international data transfers and security).”

Sanction: 30,000 Euros for lack of response to the CNIL queries, provision of inaccurate information and non-suspension of the processing.

CNIL Rejects Centralized Databases of Credit Holders in France

Experian has re-opened a debate addressed by the CNIL in a 2005 report by requesting the CNIL’s authorization for a database to be fed by credit institutions with information about their customers, the financing contracts they concluded and the status of reimbursement.

The CNIL refused to approve the project, pointing to issues such as the lack of proportionality and transparency and restating its previous finding that “only a law could specify the purposes and content of such databases … “. The CNIL has expressed reluctance in the past about positive databases and shown preference for negative databases containing only information about incidents.

---

**SINGAPORE**

By K.K. Lim

Singapore Spam Control Act 2007

Singapore’s Parliament passed the anti-spam bill on April 12, 2007, which will become law once it is published in the Government Gazette.

A spam is defined as unsolicited commercial communication, such as electronic mail and mobile text or multimedia messages, and transmitted in bulk. The message is considered as having a “Singapore linked,” (mirroring a similar spam control Australian position), if the message originates from or is received in Singapore. Parties commissioning or procuring the spam are also liable, apart from the spammers themselves.

A party can send commercially unsolicited messages if they contain the word <ADV>, have no misleading subject title or false header information and provide a prominent unsubscribe facility and con-

See, *Global Privacy Dispatches*, page 6
tactable information about the sender. The use of dictionary attack or address-harvesting software also is prohibited.

Relief is in the form of an injunction, damages suffered by the plaintiff and statutory damages not exceeding SGD 25 per message and not exceeding SGD1 million unless actual proven loss exceeds SGD 1 million. Government announcements in the interest of the public and online solicitations by religious and charities are exempted, unless the latter are selling goods or services.

New Bill on National Disease Registry

Singapore’s Ministry of Health is proposing a national disease registry bill to regulate the collection of information from patients with non-infectious diseases. The proposed bill will set out the purpose, to whom and in what form an individual’s information can be released to any research body or researcher.

The bill also will include mandatory provisions for data protection, backed by fine and or jail terms for offenders. The ministry aims to release a draft version for public feedback and comment in June 2007. The current legislation for infectious diseases such as severe acute respiratory syndrome (SARS) allows for non-consensual disclosure of patient’s information.

Singapore’s Bioethics Advisory Committee Report 2007

The Singapore Bioethics Advisory Committee (BAC) published 11 recommendations in a 48-page report to allay the public’s fear of the lack of safeguards on research subjects’ data privacy. The key recommendations are:

• Personal information such as their names and addresses should be separated from the early stage of the research to protect the identity of the person — a process known as de-identification. However re-identification is possible when needed;

• Researchers should be able to view medical records under certain conditions with permission from the supervising bodies known as Institutional Review Boards;

• Research participants can withdraw from research anytime without giving any explanation; and

• Insurance companies and employers will be prohibited from accessing predictive genetic information.

K.K. Lim is Chief Privacy Officer (Asia Pacific) at IMS Health. He may be reached at kklim@imshealth.com.

SPAIN

Spanish DPA Issues Formal Guidance on CCTV

The Spanish Data Protection Authority has issued guidance for organisations on their data protection obligations when using CCTV systems. Under European law, the processing of the image of any individual is considered the processing of personal data when that image can be linked back to an individual. At the core of the guidance is a reconciliation between the right to secure the business activities of a private company (and the citizenry at large), and the right to privacy of individuals whose images are processed through such security systems.

— Steve Kenny

UK

By David Trower

ABPI Guide on Medical Research

The Association of the British Pharmaceutical Industry (ABPI) officially launched a guide to the secondary use of patient data for medical research. These guidelines have been developed to provide the industry with advice on using and disclosing data collected for primary patient care for secondary research purposes in line with privacy and confidentiality laws.

This document was drafted by an ad hoc steering group of the ABPI, including privacy professionals from Astra, GSK, Novartis, Roche, Sanofi and IMS Health. The UK Information Commissioner, who provides a forward in the guide, approved the guidelines. The guide is available at www.abpi.org.uk/Details.asp?ProductID=315.

Article 29 Working Party and Airline Passenger Data Transfers to the U.S.

The representative group of EU Data Protection Commissioners (Article 29 Working Party) has voted in favor of including airline passenger data in the scope of the US-EU Safe Harbor data transfer agreement. This means that EU citizens will qualify for the benefits of the agreement, which includes the right to data protection in the United States.

— Steve Kenny
29 Working Party recently held a workshop relating to EU airlines’ transfer of Passenger Name Records (PNR) to the U.S. The workshop consisted of three panel sessions dealing with the legal and technical aspects involved in the transfer of passenger data to the U.S. Department of Homeland Security. The European data protection authorities highlighted the need for adequate information to be provided to transatlantic passengers to inform them of their rights and how U.S. authorities process their data. There was unanimous consent on the need to avoid a gap between expiry of the current agreement and the conclusion of a new data transfer agreement. There also was debate about the possible impact of an Automated Targeting System and whether such a tool would be incompatible with the current PNR agreement.

Royal Dutch Philips and Binding Corporate Rules

The UK Information Commissioner’s Office (ICO) has issued its second BCR authorisation to Philips. Philips’ BCR covers the processing and transfer of employees’ and clients’ personal information outside Europe. This authorisation follows on from the approval given to GE by the ICO back in December 2005 for its BCR on transferring employee data. Philips is the first application to be approved in the UK that concerns client data.

Sian Rudgard, the ICO’s spokeswoman, commended Philips for its commitment to the concept of BCR. She restated that the ICO welcomed the use of BCR by international organisations to transfer personal information.

European Court of Human Rights Issues Decision on Employer’s Monitoring of an Employee’s Personal Communications

The European Court of Human Rights in April affirmed an employee’s right to keep personal matters personal even when these intrude into the work place, subject to certain limitations. The decision applies to the 46 states of the Council of Europe. The decision in the case of Copland v United Kingdom was delivered in April 2007 and demonstrates that even before the UK Data Protection Act 1998 and the Human Rights Act 1998 came into the force in the UK, an employer’s ability to monitor an employee’s private communications and Internet use conducted over the employer’s equipment always has been very limited.

The law now specifies that unless an employer has the right policies and procedures in place the courts will not tolerate unwarranted intrusions into an employee’s personal and private life.

David Trower is the European Chief Privacy Officer for IMS HEALTH. He can be reached at dtrower@uk.imshealth.com.

ICO Addresses BCR Concerns

Following the approval of the standard form for BCR applications, a representative of the ICO has clarified some areas of potential concern for BCR applicants. Encouragingly, it is not absolutely essential to have a fully operational BCR system at the time of the application. The information commissioner realises that BCR compliance is a movable target and therefore, approvals can be given on the basis of a clear prospect of compliance.

Making an application does not open the door for an investigation into current privacy practices or potential breaches. The assessment is limited to the information provided and the ICO is aware that BCR applications are made by those who voluntarily show their commitment to comply with the law. The ICO also confirmed that it is acceptable for the main point of contact within the applicant organisation to be based outside the European Economic Area (EEA).

UK

By Eduardo Ustaran

ICO Investigates Barclays Bank

A main UK bank is at the receiving end of a privacy enquiry by the regulator. The ICO has launched an investigation into Barclays Bank following the recent BBC programme which exposed alleged breaches of customer privacy at the bank. A number of issues raised in the programme are of concern to the ICO.

One staff trainer told employees to ignore the wishes of customers who had stated that they did not wish to receive sales information or be contacted by telephone. Call centre marketing staff were told to identify themselves as “account consultants” when speaking to customers, rather than use their normal title of “sales adviser.” The film also showed call centre staff accessing customers’ accounts without a valid reason.

Eduardo Ustaran is a Partner at Field Fisher Waterhouse LLP, based in London. He may be reached at Eduardo.ustaran@ffw.com.

See, Global Privacy Dispatches, page 8
UK

ICO Finds 11 Financial Institutions in Violation of Data Protection Act

The ICO recently found 11 banks and other financial institutions in breach of the Data Protection Act. The ICO investigated a narrow aspect of compliance with the Data Protection Act, related to physical, rather than logical, destruction of identifiable information, in response to customer complaints, publicized in popular TV programs.

In accordance with its regulatory mandate, this “name and shame” exercise is intended to stimulate banks and other organizations to improve their often out-moded overall approach to information privacy. The ICO has required the CEOs of these 11 organizations, which include some of the largest banks in the world, to sign a formal undertaking to comply with the Principles of the Data Protection Act. Failure to meet the conditions of the undertaking is likely to lead to further enforcement action by the ICO and contingent reputational damage.

“The ICO investigated a narrow aspect of compliance with the Data Protection Act, related to physical, rather than logical, destruction of identifiable information, in response to customer complaints, publicized in popular TV programs.”

— Steve Kenny

UK

By Stewart Room

End of Royal Romance Leads to Calls for Privacy

The demise of Prince William’s relationship with Kate Middleton, whom many had tipped him to marry, recently dominated the media in the UK. Prince William, who is second in line for the throne, dated Middleton for four years. Not surprisingly, their relationship generated substantial media interest, reminiscent of that a quarter of a century ago, when Prince Charles was dating Lady Diana Spencer.

Earlier this year, Middleton threatened to complain to the Press Complaints Commission about press intrusion, which resulted in many newspapers announcing that they would no longer purchase paparazzi photographs of her. However, with the news of the split coming at a rather quiet time for the press, another feeding frenzy has been triggered, which already has led to further debate about the balance between the right to privacy and freedom of expression.

The privacy issue in this instance has been elevated to the highest level of political importance, with the Prime Minister, Tony Blair, calling for the press to be respectful of Middleton’s privacy. It remains to be seen whether the media will continue to operate by reference to their self-imposed embargo against paparazzi photographs or whether they will now regard Middleton as fair game now that the royals are no longer shielding her.

Stewart Room is a Partner in the Privacy and Information Law Group at Field Fisher Waterhouse Solicitors. He may be reached at stewart.room@ffw.com.

• The importance of customer notice

The rise in identity theft risks also focuses attention on the new breed of security breach issues related to the notification obligations in the event of a security breach. These laws — in place in more than 35 states with more on the way — likely will be followed in the near future by a national security breach notification standard. The widespread publicity associated with many security breaches has raised the complexity of these notice evaluations, in terms of mandating specific investigations and forcing companies to undertake a sophisticated analysis of whether notice is required (or whether it should be given even if not required), along with a host of related issues (should we provide credit monitoring, etc.). In addition, companies should be aware that regulators now are bringing the first enforcement actions related to these notice laws. In New York, the attorney general has brought an action alleging a violation of the New York security breach notification statute by CS STARS LLC, a Chicago-based claims management company (see www.oag.state.ny.us/press/2007/apr/apr26a_07.html for more information about this case).

In this context, companies should be aware of the ongoing debate about a “risk” standard for security breach notifications. The state laws vary on the standard for notification, with some states clearly limiting notice to situa-
tions where a risk of harm is “reasonable.” Other states have different (and often lesser) standards. The notice standard is a key component of the debate at the federal level. The FTC is on record as being concerned about the risk of “over-notice,” where a “too low” standard bombards consumers with multiple notices that individuals ultimately ignore or have no reasonable basis to evaluate their own potential harm.

• The crucial issue of authentication
The report focuses attention on one issue that often receives less attention — inhibiting the ability of potential identity thieves to profit from the information they have taken. If a thief obtains a consumer’s SSN, but is unable to obtain new credit cards because of the authentication practices of a credit card company, the information becomes less valuable and the losses plummet. Companies must re-evaluate their customer and personnel authentication practices. In particular, while authentication issues are not new, “better” authentication practices often have taken a back seat to improved ease of use by customers. The task force’s report shows us that companies may need to re-evaluate this balance. If identity thieves cannot use stolen information, identity theft losses decrease. This new reality must be a component of the assessment as companies review their authentication practices.

• Be aware of growing litigation
To the extent that further encouragement is needed, companies also need to be aware of the rising tide of privacy and security litigation, much of it driven by identity theft concerns. To be clear, there still is no flood of privacy and litigation. Yet, there is a consistent increase, from both consumer driven cases and litigation between companies, typically involving who is responsible for specific identity theft losses. The pending and expanding TJX breach should be watched closely as a potential tipping point. The case provides a privacy/security “Perfect Storm,” with a longstanding, ongoing security beach — apparently driven by weak security practices, resulting in substantial harm.

• Recognize that notice doesn’t get you out of litigation
When considering the litigation environment and the complexities of various notification laws, companies need to reconcile the tension between notification and the risks of litigation. It is critical to understand — and focus on — the fact that compliance with a notification law does not preclude privacy or security litigation. Instead, compliance with the notification laws is just that — compliance with these laws, without any preclusion of other enforcement or litigation activity related to the breach. The purpose of the notification laws is to permit consumers to take action proactively in an effort to prevent harm from identity theft. Obviously, these steps are designed to reduce harm. But from a legal perspective, they also can mitigate or reduce any actual damages resulting from a security breach. Proving actual damages remains a key hurdle for any plaintiff pursuing privacy or security breach litigation.

Companies providing notice should of course be aware that, in many circumstances, the notification is the first time that a consumer will learn of a security breach, and may itself lead to breach-related litigation. So, in addition to reviewing the requirements of notification laws, companies also need to consider carefully the mitigation and public relations impacts of this notification. This challenge may be particularly difficult in situations where a company’s obligation is to notify its corporate clients, rather than consumers directly. This notification process pushes the corporate client — the “owner” of the data under most statutes — to develop a notification plan that places blame on the agent. Companies need to work with their clients to develop a plan that is fair and accurate, without unduly placing blame or unnecessarily scaring consumers.

• Recognition that there are substantial weaknesses in government systems
The task force report also highlights many weaknesses in federal government security practices. The report is only the most recent description of the wide range of security flaws in governmental information systems (the GAO has a long set of reports cataloging the failures of virtually every major federal agency). These practices are even weaker at many state and local levels. In addition, there have been recent cases involving state Freedom of Information Acts. These cases demonstrate that, even where security practices are appropriate, the rules for government entities may require disclosure of information to unintended sources through routine “open government” information requests.

These concerns should motivate private companies to be wary of government information requests, and to be cognizant of these risks when providing information to governmental entities. Recognizing that there may be times when companies have no choice, companies should always review whether information must be provided, including in all instances where there are means of reducing the private information provided or otherwise encouraging additional protections for personal information about private customers and employees.

• Recognition of non-credit aspects of identity theft and other security harms
Lastly, businesses must begin to consider the range of identity theft concerns that extend beyond simple credit risks. Obviously, credit risks are significant and extensive. But as the report and other recent studies make clear, credit risks are not the only concerns with identity theft. The World Privacy Forum, for example, recently published a groundbreaking study (available at www.worldprivacyforum.org/ medicalidentitytheft.html) on the risks of medical identity theft. In addition, the FTC, in its February 2006 report, “Take Charge: Fighting Back Against Identity

See, ID Theft Task Force, page 10
Theft, “ (available at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtht04.htm), identifies the following “specific problems” that can occur in connection with identity theft:

- Bank Accounts and Fraudulent Withdrawals
- Bankruptcy Fraud
- Credit Cards
- Criminal Violations
- Debt Collectors
- Driver’s License
- Investment Fraud
- Mail Theft
- Passport Fraud
  - Phone Fraud
  - SSN Misuse
  - Student Loans
  - Tax Fraud

The FTC report details each of these harms, and describes specific means of responding to each kind of injury.

**Conclusion**

Identity theft remains a substantial problem in this country and around the world. The task force report identifies an aggressive effort to attack this problem, along with the recognition that there is a long way to go. While this government effort clearly is worthwhile, this report highlights for businesses the key areas of risk and some of the most important steps that companies can take to play their part in combating identity theft. Companies cannot view this issue as someone else’s problem. It is time for companies to take these steps to fulfill their obligation to attack the problem of identity theft.

Kirk J. Nahra is a Partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling for companies facing compliance obligations in these areas. He is chair of the firm’s Privacy Practice. He is a Certified Information Privacy Professional. He serves as the Chair of the Confidentiality, Privacy and Security Workgroup, a panel of government and private sector privacy and security experts advising the American Health Information Community (AHIC). He can be reached at knahra@wileyrein.com or 202.719.7335.

(The FTC’s Strategic Plan, called “Combating Identity Theft: A Strategic Plan,” is available at www.idtheft.gov/reports/StrategicPlan.pdf. A second volume of the report — containing a wide variety of very useful resources related to identity theft and the privacy and security of personal information, is available at www.idtheft.gov/reports/Volumell.pdf.)

This article was reprinted with permission from Wiley Rein’s Privacy in Focus newsletter (June 2007).
it is the seventh data protection principle that is immediately most relevant.

The Seventh Data Protection Principle

The seventh data protection principle is known as the security principle. It says that “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.” This obligation is expanded upon by the “interpretation” to the principles contained in Schedule 1, Part II of the Act:

“It is conventional wisdom that the Data Protection Act does not impose any reporting of security breach obligations on data controllers. However, this view is challengeable, particularly in light of the fact that the UK courts are obliged to give a purposive construction to human rights laws.”

Reporting of Security Breaches

It is conventional wisdom that the Data Protection Act does not impose any reporting of security breach obligations on data controllers. However, this view is challengeable, particularly in light of the fact that the UK courts are obliged to give a purposive construction to human rights laws.

If there is an obligation to report security breaches implied under UK data protection law, its basis would be found in the Data Protection Act’s transparency mechanisms. These mechanisms — which encompass notification, fair processing notices, processing to purpose, subject access and the Information Commissioner’s “information notice” enforcement procedure — collectively may provide the authority for the existence of a reporting obligation in UK law with a utility similar to those existing in the U.S.

One measure is contained in section 20, which creates an obligation to keep notifications accurate and up to date: notification is the process by which information about a data controller’s processing obligations is included on a publicly accessible register maintained by the Information Commissioner.

Section 18 of the act identifies the information that must be submitted with a notification, which includes “a general description of measures to be taken for the purpose of complying with the seventh data protection principle.” Section 20(2)(b) makes it clear that this general description of security measures must be kept up to date, so that the “current” measures are notified to the Commissioner.

In TK Maxx’s case, it is likely fair to assume that its current security measures are different to those in place at the time of the data thefts, which means that those changes must be notified. Furthermore — and depending on the circumstances — it might be very difficult for a controller in TK Maxx’s position to provide a useful general description without referring to the thefts; sometimes in order for the fact of change to be appreciated, the general description will require reference to the background context.

A much more convincing case for the inclusion of a breach notification obligation can be made by reference to the requirement to supply fair processing notices. This obligation arises under the first data protection principle, which says that personal data must be processed “fairly and lawfully,” as expanded by the interpretation in Schedule 1 Part II.

Paragraph 2(1) of the interpretation says that personal data is not to be treated as processed fairly unless the data controller ensures that the data subject has, is provided with, or has made readily available to them, the information identified in paragraph 2(3), which includes “any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.”

See, TK Maxx Data Theft, page 20
The April 2007 issue of Employer’s Guide to HIPAA Privacy Requirements included coverage of a breakout session at the IAPP’s 2007 Privacy Summit in Washington, D.C. in March. IAPP board member Kirk Nahra, CIPP, Partner, Wiley Rein LLP, moderated the session, which included presentations on HIPAA privacy and enforcement from North Dakota Insurance Commissioner Jim Poolman and Senior Attorney Marilou King of the U.S. Department of Health and Human Services’ Office for Civil Rights.

The article focused on the increasing number of state enforcement actions against health plans for privacy and security breaches as federal enforcement lags. Nahra provided his perspective from the private sector while Poolman and King offered the view from the state- and federal-regulator angles.

According to the article, Nahra remarked at the conference that the lack of civil penalties “has not caused a major drop in HIPAA-covered entities’ compliance efforts” but that organizations that “were very conservative in April 2003 are now somewhat less conservative.” Nahra said that given the increasing state role, as well as impending scrutiny of possible HIPAA gaps by the new Democratic-controlled Congress, health plans and other covered entities should guard against erosion of their privacy practices. He cautioned attendees, saying, “Keeping a focus of attention is, in fact, important given the potential legal and public relations impacts of a privacy or security breach.”

Poolman and King addressed the issue from the state and federal perspective, with Poolman offering advice on how insurers can work with regulators when a breach occurs, and King discussing how federal regulations are enforced.

The Practical Privacy Series, which will be held June 27-28 at the City University of New York in Manhattan, will launch this year with experts who will provide in-depth analysis and instruction on three topics: Data Breach, Pharma/Healthcare and Financial Services. SAI Global is the Platinum Sponsor of the Practical Privacy Series.

“Privacy professionals have come to rely on the IAPP for educational programming that will help them tackle the responsibilities and challenges within their companies,” said IAPP President Kirk M. Herath, CIPP/G, Associate Vice President, Chief Privacy Officer, Associate General Counsel, Nationwide Insurance Companies. “This new IAPP educational resource will send privacy professionals home with practical tips and tools they can use in their own organizations.”

The Practical Privacy Series will kick-off June 27 with a Data Breach event. Sessions are designed to provide attendees with the knowledge, skills and tools necessary to proactively identify and manage risks while effectively planning for the worst. Topics of discussion will include: case studies; updates on state and federal breach notification laws; and how to investigate and respond after an incident, deal with the legal ramifications and rebuild trust with customers and business partners.

On June 28, attendees may choose between two different events, one on Pharma/Healthcare and the other on Financial Services. The Pharma/Healthcare event will give attendees the chance to focus in-depth on the implications of electronic medical records and the impact of state laws on the pharmaceutical industry. Two other sessions offer a global focus on the transborder issues related to clinical trial data and transfer of patient information.

The Financial Services event will give attendees the opportunity to delve into various issues related to vendor management, including negotiating a contract and interaction with vendors serving the financial services industry. In the afternoon, the sessions will focus on authentication and the impact of customer trust on an organization’s bottom line.

To register for the events, or to view the brochure, visit www.privacyassociation.org.

The IAPP will offer certification testing in New York City for all three information privacy credentials on Friday, June 29, from 9 a.m. to 12:30 p.m. The examinations for the Certified Information Privacy Professional (CIPP), CIPP/G (Government) and CIPP/C (Canada) will be held at a separate location: Ernst & Young, 5 Times Square Plaza.
Alan Chapell Joins Board of Acuity Mobile

Alan Chapell, CIPP

Acuity Mobile, a provider of targeted mobile content delivery technology, recently announced the addition of Alan Chapell, CIPP, as a new board member and executive advisor. Chapell will advise Acuity Mobile on the latest issues surrounding the privacy of mobile users, with the goal of protecting the consumer’s user experience and supporting continued adoption of mobile marketing applications by users and wireless service providers.

Chapell is widely recognized as an industry leader on issues of privacy in mobile ecosystems and interactive media. Currently serving as Chairman of the Legislative and Consumer Affairs Subcommittee of the DMA’s Interactive Marketing Advisory Board, he is also Chairman of the IAPP’s New York City KnowledgeNet, Chairman of the Mobile Marketing Association’s (MMA) Privacy and Preferences Committee, and a member of the MMAs Consumer Best Practices Committee. He previously founded the privacy program at Jupiter Research and also directed Jupiter’s marketing, sales and compliance operations.

Nick Lanzer, Membership Services Assistant

Nick joined the IAPP in March as the Membership Services Assistant. In this role, he is responsible for handling logistics, including organizing member mailings and fulfilling membership requests; managing the day-to-day administration of the Continuing Privacy Education (CPE) program; and providing overall support in the membership department.

Nick is a graduate of the University of New Hampshire, holding degrees in Music Performance and Business Administration. His professional experience includes roles in customer service and hospitality.

Jennifer Taubman, Events Coordinator

Jennifer joined the conference team in May as an Events Coordinator. She primarily will work with the events team to support the IAPP’s expanding conference needs, including planning and organizing IAPP conferences. Her responsibilities also will include conference registration support and overseeing the minimum continuing legal education (MCLE) program.

Jennifer comes to the IAPP with a background in television logistics and operations. Most recently, she worked as a production coordinator for a broadcast facilities company organizing nationwide sporting and entertainment broadcasts for major television networks. Prior to that, Jennifer worked for NBC at the 2000 Summer Olympics in Sydney, Australia and the Winter Olympics in Salt Lake City, Utah in 2002. She holds a degree in Communications from Marist College in Poughkeepsie, N.Y.

New Faces at the IAPP

The IAPP is pleased to welcome two new staff members.

Alan Chapell Joins Board of Acuity Mobile

The IAPP has announced the addition of Alan Chapell, CIPP, to its board of directors. Chapell will advise Acuity Mobile on the latest issues surrounding the privacy of mobile users, with the goal of protecting the consumer’s user experience and supporting continued adoption of mobile marketing applications by users and wireless service providers.

Chapell is widely recognized as an industry leader on issues of privacy in mobile ecosystems and interactive media. Currently serving as Chairman of the Legislative and Consumer Affairs Subcommittee of the DMA’s Interactive Marketing Advisory Board, he is also Chairman of the IAPP’s New York City KnowledgeNet, Chairman of the Mobile Marketing Association’s (MMA) Privacy and Preferences Committee, and a member of the MMAs Consumer Best Practices Committee. He previously founded the privacy program at Jupiter Research and also directed Jupiter’s marketing, sales and compliance operations.

Nick Lanzer, Membership Services Assistant

Nick Lanzer joined the IAPP in March as the Membership Services Assistant. In this role, he is responsible for handling logistics, including organizing member mailings and fulfilling membership requests; managing the day-to-day administration of the Continuing Privacy Education (CPE) program; and providing overall support in the membership department.

Nick is a graduate of the University of New Hampshire, holding degrees in Music Performance and Business Administration. His professional experience includes roles in customer service and hospitality.

Jennifer Taubman, Events Coordinator

Jennifer Taubman joined the IAPP in May as an Events Coordinator. She will primarily work with the events team to support the IAPP’s expanding conference needs, including planning and organizing IAPP conferences. Her responsibilities also will include conference registration support and overseeing the minimum continuing legal education (MCLE) program.

Jennifer comes to the IAPP with a background in television logistics and operations. Most recently, she worked as a production coordinator for a broadcast facilities company organizing nationwide sporting and entertainment broadcasts for major television networks. Prior to that, Jennifer worked for NBC at the 2000 Summer Olympics in Sydney, Australia and the Winter Olympics in Salt Lake City, Utah in 2002. She holds a degree in Communications from Marist College in Poughkeepsie, N.Y.
A reader last month submitted the following question to Ask the Privacy Expert:

Q Do any global privacy laws cover the use of employee photographs for use such as security badges, organizational charts, organizational announcements, internal media or internal Web sites? Are employee photographs universally considered “sensitive personal data” or simply “personal data,” given that one may be able to deduce national origin, race, gender, and even potentially disability from a photograph?

A In general, global (non-U.S.) privacy and data protection laws are often “omnibus” laws that apply broadly whenever a company collects, uses, stores, or discloses any information about an identified or identifiable individual, including employees (personal data). As a result, employee photographs will often be regulated as “personal data” under many such laws, and will attract data protection obligations to (i) Provide affected employees with a proper notice about the intended purposes of use and the like, (ii) Maintain reasonable security measures to protect the data, (iii) Update registrations with data protection authorities to reflect the use of the data, (iv) Ensure adequate protection for international transfers of the data, and (v) Address other requirements. A more difficult question is whether employee photographs would be “sensitive” personal data entitled to heightened protections (i.e., express consent requirements), particularly if the photographs reveal national origin, race, disabilities, etc.

We raised this question with several of our privacy practitioners in jurisdictions around the world, and have summarized their responses below. As is evident, the answers vary depending on the specifics of the local laws, as well as the intended purposes of use of the photographs and other factors. Naturally, with any good data protection or privacy question, the responses reveal that the other applicable legal requirements — beyond privacy and data protection — will bear on the question as the company works its way toward finding an appropriate regulatory solution to its planned activities with employee photographs.

— Brian Hengesbaugh, brian.hengesbaugh@bakernet.com, Baker & McKenzie (Chicago)

Argentina

The Argentine Data Protection Law defines personal data as any information related to natural persons or legal entities. It could be argued therefore that personal data includes “photographs,” and when such photographs disclose information about race or ethnic origin, health or disability information, such data arguably may constitute “private data,” which would be subject to heightened restrictions under the law. The company therefore may need to obtain consent from affected employees, and indeed may wish to consider taking steps to avoid capturing or using employee photographs that reveal such private data. The Argentine Civil Code provides protection against arbitrary interference with the private life of others or publishing images that harm others’ customs or feelings. An employee could therefore seek redress under these statutory protections or the data protection law to the extent the employee considers that he or she is adversely affected by a photograph that is published to a wide audience through a company’s Web site, intranet, newsletter or in a press release or announcement.

— Marcelo Slonimsky, Marcelo.Slonimsky@bakernet.com.ar, Baker & McKenzie (Buenos Aires)

Belgium

In Belgium, an employee photograph would constitute personal data. To the extent the photograph reveals race or ethnic origin, health or disabilities, or the like, such a photograph would likely be considered “indirectly sensitive” personal data. In other words, employee photographs may not rise to the level of “sensitive” personal data as long as the purpose of processing is not related to the potentially sensitive character of the data. For instance, if the purpose for processing the photographs is ethnic screening, those photographs would be considered sensitive personal data, and will require express consent or may be entirely prohibited. In contrast, the processing of such photographs will not be considered as

— Daniel Fesler, daniel.fesler@bakernet.com, Baker & McKenzie (Brussels)
processing of sensitive data if they are processed for necessary work-related identification purposes.

— Daniel Fesler, Daniel.Fesler@bakernet.com, Baker & McKenzie (Brussels)

France

Under the French Data Privacy Law, “personal data” is defined to include any information relating to an identified or identifiable natural person (data subject). Such definition is broad enough to cover individual photographs and images that allow directly or indirectly the identification of a natural person. As early as 1994, the French Data Protection Authority (the CNIL) indicated that images captured by a video camera in a monitoring system should be regarded as personal data. In 2005, the CNIL again confirmed that: (i) Individual images are protected by the fundamental rights to privacy and article 9 of the French Civil Code and (ii) They constitute also personal data as they allow the identification of a natural person. The CNIL also noted that photographs may not necessarily constitute “sensitive” personal data. However, as mentioned by others, if the photographs are used by the company for the purpose of identifying an individual’s race or ethnic origin, or the like, it would be possible to argue that such photographs do indeed constitute “sensitive” personal data that attract express consent requirements if not entire prohibitions on processing.

— Denise Lebeau-Marianna, Denise.Lebeau_Marianna@bakernet.com, Baker & McKenzie (Paris)

Germany

In Germany, employee photographs generally constitute “personal data” that falls within the scope of the German Data Protection Act. Such photographs also generally will constitute “sensitive” personal data where the race or health (i.e., disabilities) of a person can be discerned, and therefore such processing may attract an express consent requirement. In addition, to the extent the photographs will be published internally to a wide audience (i.e., through organizational charts, company announcements, or internal Web sites) such publication is likely to also fall under the German Act on Artistic Works. This act generally requires the consent of the person prior to publishing his or her photograph.

— Christoph Rittweger, Christoph.Rittweger@Bakernet.com, Baker & McKenzie (Munich)

Italy

The Italian data protection authority recently issued guidelines on the processing of employee personal data, and expressly mentioned photographs as one form of “personal data” that a company would process about its employees. In general, a company only will be able to use and disclose such photographs internally without consent where the company can justify such processing as necessary for the performance of obligations resulting from the employment contract. If the photographs are to be published externally to customers or third parties, consent generally will be required. When photographs disclose race, ethnic origin, or health or disabilities, they qualify as “sensitive” personal data, and will attract an express consent requirement in any case.

— Giovanni Parrillo, Giovanni.Parrillo@bakernet.com, Baker & McKenzie (Rome)

Spain

In Spain, employee photographs are considered personal data because they are related to identified employees. The Spanish Data Protection Agency has yet to address the issue of whether photographs are sensitive personal data. In general, an argument can be made that photographs should not be considered “sensitive” personal data (even if they reveal race, ethnic origin, and the like) so long as the photographs are not used for the purpose of identifying or processing such “sensitive” personal data, but rather for customer human resources and organizational security purposes. If the employee photographs are used beyond what is necessary for the employment relationship, or if the posting of the employee photographs can be regarded as an international transfer of data, then the employees’ consent may be required.

— Norman Heckh, Norman.Heckh@bakernet.com, Baker & McKenzie (Madrid)

See, Ask the Privacy Expert, page 16
United Kingdom

In the United Kingdom, the courts have determined that photographs and images of people are capable of being personal data (Durant v Financial Services). In particular, where the name and image of a person are linked — or are capable of being linked — then the person can be identified and the image should be regarded as personal data under the UK Data Protection Act (1988). The Information Commissioner’s Office (ICO) has taken a pragmatic approach on the issue of whether photographs are “sensitive” personal data by saying that while an image might indeed constitute sensitive personal data, the depiction of someone’s skin color is not a clear indication of ethnicity and should not, by itself, be regarded as sensitive personal data. However, if an employer has other data about an employee, which coupled with the photo of the employee could confirm the sensitive information depicted by the image then, in theory, both sets of data should be treated as sensitive personal data. In practice, though, (and until the courts provide a clear ruling on this point), employers who do not treat photos as sensitive personal data can take some comfort from the ICO’s practical view.

— Christina Demetriades, Christina.Demetriades@bakernet.com, Baker & McKenzie (London)

This response represents the personal opinion of our experts (and not that of their employer), and cannot be considered to be legal advice. If you need legal advice on the issues raised by this question, we recommend that you seek legal guidance from an attorney familiar with these laws.

Attention IAPP Members — We Need You!

The IAPP is looking for international contributors to our new Global Privacy Dispatches column, a new monthly feature that will provide brief updates on privacy and security stories unfolding in countries around the world.

The IAPP also is looking for copy in an upcoming issue that will cover the developing trends in privacy enforcement and litigation. We are seeking ideas and writers for this upcoming issue.

If you would like to contribute to Global Privacy Dispatches or have enforcement or litigation story ideas, please email ann.donlan@privacyassociation.org.
The PRACTICAL PRIVACY Series
June 27-28
Data Breach
Financial Services
Pharma/Healthcare

3 EVENTS • 2 DAYS • 1 CITY

NEW YORK

To learn more about these exciting new events visit us at privacyassociation.org

Made possible by our Platinum Sponsor:

Gold Sponsors:

iapp
international association of privacy professionals

FPO
Pick up camera ready ad from May 07 Advisor
Congratulations, Certified Professionals!

The IAPP is pleased to announce the latest graduates of our privacy credentialing programs. The following individuals successfully completed the CIPP and CIPP/G examinations held in March 2007 in Washington D.C.

Aref Alvandy, CIPP/G
Maureen Campbell, CIPP
David G. Carpenter, CIPP
Kathleen Mary Carroll, CIPP
Paul E. Clement, CIPP
William H. Domaine, CIPP/G
Paul M. Dempsey, CIPP
Jon-Eric Dentz, CIPP
Sandra A. Donsett, CIPP/G
Sonia I. Flores, CIPP
Kat V. Foy, CIPP/G
Katherine Rawls Foster, CIPP
Pamela S. George, CIPP
Marcia L. Greer, CIPP
John Mark Hopkins, CIPP
Sandra P. Jenkins, CIPP/G
Ralph Johnston, CIPP/G
Kevin B. Kenan, CIPP
Katrina Elizabeth Kletchy, CIPP/G
Marina R. Klochan, CIPP
Holly Noel Korzilius, CIPP
Gregory Lackey, CIPP
Christopher Lanzilotta, CIPP
Dimo Michailov, CIPP
Robert D. Mims, CIPP
Scott Orlo Murdoch, CIPP
Victoria Eva Newhouse, CIPP/G
Sarah Kristin Othhoff, CIPP
James T. Parker, Jr., CIPP
Chris A. Peters, CIPP
Kimberly Quinn, CIPP
Shahir S. Shah, CIPP
Cheston Olamide Sobande, CIPP/G
Kristin I. Sostrom, CIPP
Rebecca Lee Springer, CIPP
Kanakaraj Pillai Subramanian, CIPP
Stefani Vetter Watterson, CIPP
Jesse H. Webb, CIPP
Katherine White, CIPP/G
Matthew Paul Widick, CIPP
Buzz Willis, CIPP/G
James R. Wyne, CIPP
Brian J. Zwit, 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!

Privacy News

Paula Bruening Appointed Deputy Executive Director for The Center for Information Policy Leadership at Hunton & Williams

Paula J. Bruening has been appointed Deputy Executive Director for The Center for Information Policy Leadership and Senior Policy Advisor at Hunton & Williams LLP. Bruening joins the firm after having served as counsel at the Center for Democracy & Technology, a nonprofit public interest organization, where she focused on cyber-privacy issues.

“Paula brings the special skills necessary to create collaborative solutions in an information age,” said Marty Abrams, The Center’s Executive Director. “She understands the intersection between policy and technology, which is so important when looking at emerging privacy issues including those arising in technologies such as RFID and social networks.”

Fireman’s Fund Offers Data Compromise Insurance for Businesses

Fireman’s Fund Insurance Company has introduced Data Compromise, coverage that helps businesses respond quickly and effectively to a data breach, covering the costs to notify affected individuals and providing a suite of services, from credit report monitoring to identity theft restoration case management.

The service includes legal consulting, customer notification services and credit monitoring as well as identity restoration for customers, employees and others affected by a data breach.

“Many state laws require businesses to notify individuals whose information has been compromised, and it’s only a matter of time before a Federal law is enacted,” said Mike Roney, Senior Director, Commercial Business at Fireman’s Fund. “In order to help our policyholders remain compliant, as well as maintain goodwill with their valuable customer base, we have created our Data Compromise coverage, which provides assistance throughout the data recovery process.”
DHS Privacy Office Seeks Increased Funding

Hugo Teufel, CIPP/G, Chief Privacy Officer for the U.S. Department of Homeland Security (DHS), has asked the House Appropriations Subcommittee on Homeland Security for $5.122 million for 2008 — a 16 percent budget increase. The additional funding would be used to hire additional employees to address privacy issues and freedom of information issues.

In his written testimony, Teufel states, “Both the privacy and FOIA sides of the office have experienced significant growth over the past four years of the office’s existence. Thus, on the privacy side, additional positions are needed in order to conduct the increasing number of PIAs [privacy impact assessment], SORNs [system of records notices], and internal privacy audits, as required under the E-Government Act and Homeland Security Act. As such the resources currently allocated to the Privacy Office must be increased sufficiently to match the expanded reach and operation of both the Privacy Office’s functions.”

Lucy Thompson, CIPP/G, Appointed Consumer Privacy Ombudsman

Lucy Thompson, CIPP/G, was recently appointed Consumer Privacy Ombudsman by the U.S. Bankruptcy Court in the Eastern District of Virginia to oversee the sale of consumer records in the Storehouse, Inc. bankruptcy case. This is only the fourth such appointment nationwide.

Thompson currently is a Senior Principal Engineer, Information Security and Privacy Advocate at global IT company Consumer Sciences Corporation. She previously served as a U.S. Department of Justice attorney in the Criminal and Civil Rights Divisions.

Privacy Classifieds

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

SENIOR PRIVACY ANALYST II
Carolinas HealthCare System
Charlotte, N.C.

PRIVACY & DATA PROTECTION SENIOR MANAGER
Deloitte & Touche
Chicago, Ill. and Minneapolis, Minn.

DATA & PRIVACY PROTECTION CONSULTANT — MANAGER — SR. MANAGER
Deloitte & Touche

PRIVACY COMPLIANCE MANAGER
KPMG
Montvale, N.J.

PRIVACY PROJECT MANAGER
Ernst & Young
New York, N.Y.

SENIOR PRIVACY & COMPLIANCE SPECIALIST
Iron Mountain
Boston, MA

PRIVACY OFFICER, SENIOR DIRECTOR, CORPORATE COMPLIANCE
State Street Corporation
Boston, Mass.

INVESTIGATOR 2, CORP INVESTIGATIONS
T-Mobile
Bellevue, Wash.

PRODUCT COUNSEL, PAYMENTS
Google Inc.
Mountain View, Calif.

PRODUCT COUNSEL
Google Inc.
Mountain View, Calif.
The argument for inclusion of a breach notification requirement is simple: Once the data controller has suffered a TK Maxx-style security breach, it cannot be fair to the data subject for the controller to continue processing without notifying them of it, because the basic parameters of the processing operation have changed. Furthermore, serious failures of security do influence data subjects’ decisions about the continuance of business with controllers, particularly where the controller cannot guarantee that it has resolved all outstanding issues, or where there is doubt about the parameters of the breach. So, in the immediate aftermath of a security breach, it can be argued that the controller’s processing operations are not the same as those communicated to the data subject prior to the start of processing. This also applies to circumstances in which the controller indicated the processing would start or led the data subject to believe that its security met the standards required by the seventh data protection principle. But after a security breach, the accuracy of the controller’s original statement or representation is undermined, meaning that the processing operation has changed, going from purportedly secure to evidently insecure.

**Damages**

TK Maxx already is facing massive class actions in the U.S. In April, the Massachusetts Bankers Association brought a class action lawsuit, related to the expense of reissuing payment cards. The Arkansas Carpenters Pension Fund also has sued for TJX’s failure to divulge more details about the security breach.

In the UK, the Data Protection Act permits damages claims. Section 13 says that “an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this act is entitled to compensation from the data controller for that damage.” In cases of damage, the individual also can recover compensation for distress.

The courts already have held that “damage” for the purposes of section 13 means pecuniary loss (see Johnson v. Medical Defence Union, Court of Appeal 28th March 2007 and Campbell v. Mirror Group Newspapers, High Court of Justice Queens Bench Division 27th March 2002). As a result, it will be necessary for a claimant to show financial loss before any compensation claims can be launched in the UK. This hurdle to recovering compensation is a low one in the circumstances of this case, as any TK Maxx customer who seeks to put in place new banking facilities as a result of the security breach will incur pecuniary loss, even if it is merely the cost of a few telephone calls, stamps and envelopes.

This low threshold to a damages claim must be very worrying for TK Maxx, as it opens up the much wider claim for compensation for distress. In the Johnson case mentioned earlier, the trial judge held that a £10.50 financial loss claim (just over U.S. $20) triggered a £5,000 (about U.S. $10,000) compensation award for distress. Multiplied up it is obvious that TK Maxx faces a huge potential compensation claim, particularly if the UK legal profession mirrors its U.S. counterpart and brings forth a class action.

Stewart Room is a Partner in the Privacy and Information Law Group at Field Fisher Waterhouse Solicitors. He is the author of ‘Data Protection and Compliance in Context’ (November 2006 ISBN 1-902505-78-6) and the Chairman of the National Association of Data Protection Officers. He can be reached at stewart.room@ffw.com.