Avoiding the Dumpster Spotlight

By Luis Salazar, Elise Berkower, and Greg Dean

It seems that you cannot swing a credit report these days without hitting a local news crew covering a story about records carelessly thrown out in a local dumpster. In fact, a by-product of the sub-prime meltdown has been mortgage companies going out of business and leaving loan applications containing personal financial information in the trash. These stories are enjoying media attention because they rightfully concern consumers, who have an expectation that their private data are being safeguarded and not tossed in the garbage for anyone to grab.

But it must also be troubling to business and privacy professionals, too, at least judging from the nearly 65 participants at the preconference session entitled “Data, Data, Everywhere: Transferring, Selling, Trashing, or Destroying Data” at the IAPP’s annual Privacy Summit in March. The session covered the problem of disposing of data, both in the ordinary course and in the more complex situation presented by troubled companies and companies in mergers and acquisitions. Here, in a vastly more concise form, are some of the highlights and best practices offered during that session.

Legal Requirements

From a legal perspective, there are various federal and state laws and regulations that require records containing sensitive consumer information to be properly cared for and disposed of. More specific laws on the disposal of

The Privacy Challenges of U.S. Fusion Centers

By Rebecca Andino, PMP, CIPP/G

Consider these scenarios:

Scenario #1: Officials suddenly notice a pattern of individuals trespassing in unusual areas of a subway. They take action and successfully prevent a terrorist attack, saving dozens of lives.

Scenario #2: A large corporation partners with a state fusion center and quietly uses its databases to screen prospective employees. When the media reports this, citizens are outraged, authorities and officials are scrambling, and Congress is planning hearings.

These are just two examples of the opportunities and privacy risks involved in U.S. fusion centers.

Fusion centers have existed in various forms for decades, but since 9/11, their role has expanded and evolved. Recent actions, such as the Implementing Recommendations of the
Springtime at 43 degrees north finds Canadians shedding their parkas and squeezing every last ray of sunlight possible from the day. That’s what we found at the IAPP’s first-ever Canadian Privacy Summit in Toronto May 21-23, where hundreds of lively Canadian privacy pros gathered to learn, network and become privacy certified.

The three-day event was a big hit in this country whose privacy policies other nations covet. Privacy pros came out of the trenches to hear, share and connect on privacy issues large and small alongside Canada’s privacy commissioners and experts from across the country.

But all good things must end, and leaving Toronto on a high note was the only way to leave such a great city. Today, the full heat of almost-summer is upon us, while our friends in the southern hemisphere look ahead to their winter season. Although our climates differ, the privacy issues we contemplate on a daily basis are the same.

Another day, another stolen laptop.

It seems I’ve just digested the news of the UnitedHealthcare data breach that resulted in the identity thefts of 155 University of California-Irvine graduate students, yet as I write, another massive breach is making headlines, this time at Stanford University, where the personal information of tens of thousands of current and former employees has been put at risk. And to think that these are just the breaches we hear about... A recent Gartner study suggests that only a small percentage of retailers hit by information breaches actually notify the public of the incident. There is something tiring about weekly data breach headlines. Equally as discouraging is the annual report of the office of the Canadian privacy commissioner, which highlights the fact that despite the notoriety these breaches bring, a great many organizations still haven’t taken basic measures to protect private data.

There is no end in sight to the issues we all work so hard to resolve. And, like poison ivy bubbling just under the surface of the skin, new ones come into the fray every day. Locational privacy was in the news again this month, and is bound to become a bigger topic as researchers continue their efforts in this area. We’ll examine this topic in an upcoming issue of the Privacy Advisor.

Meanwhile, in this month’s issue we’re excited to bring you an insightful look at the history and privacy implications of U.S. Fusion Centers (did you know almost every state has one?), and a story on practical and important steps you can take to make your organization rock solid when it comes to data destruction.

I hope you enjoy this issue of the Privacy Advisor.

J. Trevor Hughes, CIPP
Executive Director, IAPP
sensitive data apply, too. To start, many laws require financial institutions and other businesses to provide adequate security, such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), as well as the security-related regulations issued in connection with them. The obligations imposed by these and similar laws do not end at the dumpster’s edge. On the contrary, information must be safeguarded at all times.

In addition, there are other laws and regulations that focus on the disposal of sensitive information. For example, the Fair and Accurate Credit Transactions Act, or FACTA, directed the Federal Trade Commission (FTC) to enact rules and regulations governing the disposal of credit reports. In 2004, the FTC promulgated what has become known as the “Disposal Rule.” The Disposal Rule requires businesses to take “reasonable measures” to protect against unauthorized access to, or use of, customer information in connection with its disposal, as well as other documents containing information derived from consumer reports.

As covered by the rule, “disposal” is a broad concept, which encompasses abandoning, selling, donating, or transferring, any document or media containing consumer information. Thus, computer equipment, PDAs, and discs, are included. “Reasonable measures” include conducting due diligence on a disposal company, ensuring that papers containing customer information are burned, pulverized, or shredded, and that electronic files or media containing customer information are properly destroyed or erased. Reasonable measures include implementing policies and monitoring compliance to ensure the rule is followed.

States have also jumped into this area with different approaches. For example, the state of Texas requires businesses to “destroy or arrange for the destruction of customer records containing sensitive personal information.” “Destroy” is further explained to be shredding, erasing, or otherwise modifying a document to make it unreadable. Other states, such as New York, have taken a more precise approach, requiring the destruction of documents that contain specific customer information, such as Social Security numbers, driver’s license numbers, mothers’ maiden names and account numbers.

Penalties for non-compliance can be significant, including injunctive relief barring further violations, post-violation auditing requirements, fines and, in some cases, criminal sanctions.

Enforcement Efforts

Regulators at all levels are strictly enforcing these laws. In December 2007, the FTC brought an enforcement action against American United Mortgage Company for failure to abide by the disposal rule, resulting in a fine of $50,000, an obligatory initial and subsequent biennial assessment reports from a third-party auditor, and other compliance monitoring.

Likewise, the state of Texas has brought five separate enforcement actions under its own state law, mostly as a result of documents improperly disposed of in dumpsters.

See, the Dumpster Spotlight, page 4

---

The Dumpster Spotlight

continued from page 1

Luis Salazar

Elise Berkower

Greg Dean
Strategies for Compliance

Many garbage disposal companies began offering document destruction services as these disposal rules and regulations began to drive greater business demand. But garbage disposal companies are not in the security business, and they may fail to take measures necessary to meet the Disposal Rule or other legal requirements. Therefore, businesses must be certain to take careful steps to choose the right service provider and comply effectively.

To start, businesses should conduct due diligence before entering an agreement with the disposal company, and make sure to:

- **Check References.** Ask a potential service provider for references from reputable companies that use its services and make sure to check and document your contacts with those references.
- **Check Certifications.** The National Association of Information Destruction (NAID) has a Certification Program for Information Destruction Companies to ensure the quality of their disposal programs. Although not a guarantee, a NAID or similar certification is a strong sign that a company takes its responsibilities seriously. Additionally, in October 2008, New York Business Law 899-bbb will become effective. This law requires disposal companies to undergo criminal and other background checks as part of the process to obtain licenses authorizing them to conduct a disposal business.
- **Conduct a Site Check.** Consider visiting the disposal company’s site. Is there security to prevent entering into the disposal area? Are logs kept? Are there security cameras? Is the unloading of documents—shredded or yet to be shredded—taking place out in the open, where the wind can blow them around the disposal yard? Much can be learned from a site visit during the due-diligence period.
- **Ask for Written Policies.** Ask your prospective disposer to provide copies of its internal policies regarding handling of documents to be shredded and their subsequent disposal.
- **Read the Contract.** Be sure to read the proposed service contract and understand what obligations the disposal company agrees to undertake, including the security level of shredding, subsequent recycling or disposing of the shredded material, indemnification and other provisions.
- **Bonding/Insurance.** Disposal companies should have adequate bonding and insurance in the event something goes wrong. Be sure to ask for the declaration page, demonstrating the validity of any insurance.

**Next Steps**

Once you have chosen a disposal dealer, there are still a number of internal steps businesses must take to ensure that the process works. Consider the following:

- **Make Containers Convenient.** Make sure to give your employees every reason to use the shredding disposal bin by making it as convenient as possible.
- **Make it Enforceable.** Proper disposal of sensitive documents is a vital part of your business. Make sure that compliance is mandatory and is clearly spelled out in your internal employee policies. Your policies should spell out levels of discipline, up to and including termination, for non-compliance. And of course, be certain to consistently enforce that policy.
- **Establish the Chain of Custody.** Businesses should specify individuals responsible for documents throughout the disposal chain of custody. That is, once documents are placed in the shredding bin, it should be clear whose responsibility it is to make certain that the documents are properly and securely transported to the next step in the process.
- **Determine the Shred Size.** Decide the level of security you wish to achieve in the shredding process. Low security, or simple strip-shredding, may not be suitable for many businesses. Instead, cross-cut, particle-cut, or “granulation”—each providing greater level for disintegration—may be more appropriate. In Europe, there are specific “DIN” standards that apply.
- **Obtain Certificate of Destruction.** Be certain to obtain a certificate of destruction from the disposal company confirming it disposed of the documents. That certificate is not a free pass, but obtaining it is evidence that
the business is being diligent about its destruction process.

• Random/Regular Site Visits. Even after a disposal system is up and running and a business is regularly using a disposal service, it still makes sense to schedule random but regular site visits to your disposer. Once again, look for the same tell-tale signs that the job is being properly conducted—adequate security, backup papers strewn about the yard, and the like.

A similar due diligence and policy scheme should be enacted with electronic devices and media as well. Whether you are hiring a service for such disposal, or simply acquiring hardware and software to conduct the disposal internally, be sure to conduct adequate due diligence, establish policies to enforce disposal mechanisms, and audit your disposal efforts to ensure effective compliance.

An effective disposal program is an indispensable part of a business’ data privacy efforts; not only will effective compliance ensure that applicable legal requirements are met, but it will prevent the potential damage from having shoddy disposal efforts broadcast on the evening news.

**U.S. Fusion Centers**


Fusion centers may increase public safety because they facilitate information sharing between different levels of government and between the public and private sectors. A fusion center, as defined by the Department of Justice (DOJ) in the *Fusion Center Guidelines*, is a “collaborative effort between two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity.”

However, complex lines of authority, the variety of implementations and the fact that 58 centers are already fully operational, create privacy challenges and opportunities.

**Current Status of Fusion Centers**

According to the interactive map on the American Civil Liberties Union (ACLU) Web site, fusion centers exist in every state except Idaho and Hawaii. The Congressional Research Service (CRS) report “Fusion Centers: Issues and Options for Congress,” reports that the majority are co-located with a state police headquarters; fewer than 20 percent of fusion centers are regional or local in jurisdiction.

“Fusion centers exist in every state except Idaho and Hawaii.”

Fundamentally, fusion centers are not federal entities; they are operated by state, regional, or local law enforcement entities. According to the CRS report, the Department of Homeland Security (DHS) has provided about $380 million in funding since 2001. It estimates fusion centers are funded about 80 percent by states and 20 percent by the federal government. Each fusion center has a different funding and governance structure. As a result, each fusion center is subject to a unique combination of state and federal laws governing criminal intelligence information collection and handling and information sharing.

There are numerous federal touchpoints to fusion centers. The official federal liaison to fusion centers is the State and Local Program Office in the DHS. The DHS provides staffing, technical, and privacy and civil liberties training to fusion centers and collaborates with the Global Justice Information Sharing Initiative (“Global”), a DOJ entity, to deliver training. In addition, the FBI provides special agents and other staff; more than a dozen fusion centers are collocated with FBI entities. Finally, because fusion centers are part of the Information Sharing Environment (ISE), the Program Manager of the ISE,
U.S. Fusion Centers  continued from page 5

from the Office of the Director of National Intelligence (ODNI), provides the overall information sharing framework, privacy guidance and resources.

The key privacy challenges related to fusion centers stem from the complex governance structures, and the need to apply the appropriate levels of transparency to this high-profile security mission.

Complex Governance

There is no lack of guidance; the federal government has provided substantial privacy guidelines and resources to fusion centers, including those listed in the sidebar. Instead, the challenges are related to how the guidance will be implemented, and the roles, responsibilities and accountability assignments.

Currently, there is forward momentum and cooperation between Federal agencies and fusion centers, demonstrated by joint participation in the DHS Data Privacy and Integrity Advisory Committee, joint press releases and well-attended fusion center conferences. However, it is a work in progress; the relationships between DHS and each of the 58 fusion centers are still being established. The agencies are currently in the process of defining how privacy and civil liberties guidance provided from the federal government will be ensured.

Federal agencies must use influence, not authority, to achieve fusion center compliance with the federal privacy guidelines. The ISE guidelines do not apply to fusion centers, but do require federal entities to ensure that any fusion center with which they share information has privacy protections that are at least as comprehensive as the ISE guidelines. The DOJ Fusion Center Guidelines are completely voluntary, although, according to a DHS official, all fusion centers have agreed to follow them.

Typical non-compliance actions, such as withholding funding or revoking network connectivity would halt information sharing, harming the overall counter-terrorism mission. Instead, the federal government has engaged fusion centers in a collaborative partnership to achieve alignment with the guidelines. DHS, DOJ and the ISE are offering training and other resources such as sample privacy policies and procedures, through the Global Fusion Process Technical Assistance Program.

Transparency and the Fair Information Practices

The second major privacy challenge of fusion centers is to achieve the appropriate balance between transparency and the protection of sensitive, mission-critical information.

As non-federal entities, fusion centers are not bound by the Privacy Act or E-Government Act, although the DHS and National Governors Association recommend all fusion centers develop a Privacy Impact Assessment (PIA) as a privacy management tool. The DHS is providing PIA training and assistance to each of the fusion centers through the Global program. Whether the PIAs will be made available to the public is up to the leadership of each individual fusion center.

At the federal level, DHS is required to perform an overall PIA on fusion centers. In the 9/11 Act, Congress directed the DHS privacy officer to deliver a Concept of Operations that includes an initial privacy and civil liberties assessment by November 2007, and a PIA on August 8, 2008. The PIA is currently in draft form and under review for submission to Congress.

All fusion centers are different. Some are extremely open about their information practices, even providing their standard operating procedures to the public. Others are not as open. Privacy issues will be discussed in each fusion center’s PIA, if fusion centers choose to create them, and will address their approach to the Fair Information Practices (FIPs). Issues include:

Openness

Many fusion centers have not shared with the public what databases they use. This was demonstrated in an April 2, 2008 article in The Washington Post titled “Centers Tap into Personal Databases.” It revealed that several fusion centers in the northeast have access to millions of people’s information including unlisted cell phone numbers, insurance claims, driver’s license photographs and credit reports.

Although these resources are common to state and local law enforcement agencies, the fact that fusion centers had access to such a wide variety of commercial databases was previously unknown to the public.

In March 2008, EPIC filed a Virginia FOIA lawsuit against the Virginia State Police for refusing to provide information on meetings with the DHS and the DOJ regarding funding, operations and information-sharing governance.
Collection

While many fusion centers do adhere to 28 CFR, Part 23, which requires “reasonable suspicion” in collecting information on individuals, some fusion centers may not. PIAs, if developed and published, will describe the conditions under which personal information is collected.

In its article “What’s Wrong with Fusion Centers,” the ACLU equates the fusion process to data mining on innocent individuals, a practice they claim is both unfair and ineffective for predicting or preventing acts of terrorism.

Use

To comply with the FIPs, fusion centers should ensure that personal information will be shared with other entities only for its lawfully-stated purpose. Fusion centers will share information with the private sector. In a warning similar to the example scenario at the beginning of this article, the ACLU cautions that protections against improper private sector use must be built in to ensure people will not be unfairly fired from a job, evicted from an apartment, denied a loan or otherwise unfairly treated based on information shared between a fusion center and the private sector.

Individual Participation

Individual participation—in particular, redress—in fusion centers is challenging, for two reasons. First, information collected about individuals in fusion centers is often exempt from State Freedom of Information laws, so limited if any individual participation is possible. Second, the complex network of fusion centers and the federal government may make it particularly difficult for an individual to determine which entity “owns” his or her information in order to submit a redress request to that entity.

The Fusion Center Guidelines do not recommend a specific redress policy, but state that fusion centers should consider implementing the Fair Information Principles, including the “Individual Participation” principle. Section 8 of the ISE’s 2006 Privacy Guidelines directs federal agencies that participate in the ISE to implement redress processes.

Accountability

Who is ultimately accountable for protecting privacy? Larry Ponemon of The Ponemon Institute asked this question at the September 19, 2007 DHS Advisory Committee meeting. One panelist responded that the fusion center director would be responsible and accountable; another said the “buck stops” with the governor of each state. Because all states have different governance models and internal oversight processes, they said there is no “cookie-cutter approach.”

Next Steps

The DHS Privacy Office is completing the fusion center PIA and will submit it to Congress. The majority of DHS PIAs are made available to the public, although the DHS has not stated whether this PIA will be released. The DHS is in the process of identifying the privacy point of contact at each fusion center; representatives are traveling to meet individuals at each fusion center. The DHS and Global will continue to deliver privacy and civil liberties training to analysts assigned to fusion centers. As one DHS official stated, “Protecting privacy in fusion centers is a continuous process. There is no finish line.”

Rebecca Andino, PMP, CIPP/G, is president and founder of Highlight Technologies, a firm providing program management and privacy consulting services to national security programs. Contact Rebecca Andino at randino@highlighttech.com or 202-271-0469.

Privacy Resources related to Fusion Centers

<table>
<thead>
<tr>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLU Map of Fusion Centers</td>
</tr>
<tr>
<td><a href="http://www.aclu.org/privacy/gen/fusion_map/">www.aclu.org/privacy/gen/fusion_map/</a></td>
</tr>
<tr>
<td>DOJ Fusion Center Guidelines</td>
</tr>
<tr>
<td><a href="http://www.it.ojp.gov/fusioncenter">www.it.ojp.gov/fusioncenter</a></td>
</tr>
<tr>
<td>DHS Data Privacy and Integrity Advisory Committee Meetings and Minutes</td>
</tr>
<tr>
<td><a href="http://www.dhs.gov/xinfoshare/committees">www.dhs.gov/xinfoshare/committees</a></td>
</tr>
<tr>
<td>CRS Report for Congress: Fusion Centers: Issues and Options for Congress</td>
</tr>
<tr>
<td><a href="http://opencrs.com/document/RL34070">http://opencrs.com/document/RL34070</a></td>
</tr>
<tr>
<td>ISE State, Local and Tribal Privacy and Civil Liberties Guidance</td>
</tr>
<tr>
<td><a href="http://www.ise.gov/pages/privacy-slt.html">www.ise.gov/pages/privacy-slt.html</a></td>
</tr>
<tr>
<td>ISE Fusion Center Web Site</td>
</tr>
<tr>
<td><a href="http://www.ise.gov/pages/partner-fc.html">www.ise.gov/pages/partner-fc.html</a></td>
</tr>
<tr>
<td>Illinois Criminal Justice Information Authority: “Privacy Smchprivacy?”</td>
</tr>
<tr>
<td>Drafting Privacy Policy in an Integrated Justice Environment (and why</td>
</tr>
<tr>
<td>it’s important)</td>
</tr>
<tr>
<td><a href="http://www.icjia.state.il.us/iijis/public/index.cfm?metasection=tools&amp;metapage=privacyFront">www.icjia.state.il.us/iijis/public/index.cfm?metasection=tools&amp;metapage=privacyFront</a></td>
</tr>
<tr>
<td>EPIC Web Site on Information Fusion Centers and Privacy</td>
</tr>
<tr>
<td><a href="http://epic.org/privacy/fusion/">http://epic.org/privacy/fusion/</a></td>
</tr>
</tbody>
</table>
An Introduction to Privacy Enhancing Technologies

By Steve Kenny

As increasing amounts of personal data are being held, the risk of breaching data protection legislation and regulation has grown ever greater. At the same time, data protection laws are tightening across the world in response to consumers’ and citizens’ concerns. As part of a broader information governance strategy, some organisations are making greater use of more automated controls to manage data protection.

More than a decade ago, the Dutch and Ontario Data Protection Authorities recognised the role of technology in protecting privacy and coined the term Privacy Enhancing Technologies (PET). Today, European Data Protection Authorities routinely refer to PET as an approach to help achieve compliance with data protection legislation. Here, Steve Kenny, former PET expert with the European Commission and the Dutch regulator, provides a quick introduction to PETs and how they can contribute to the management of privacy risk.

There are no uniform definitions of PET; but it typically refers to the use of technology to help achieve compliance with data protection legislation. The business case for adopting PETs is frequently not limited to the confidentiality of personal information, for example many of the technologies referred to as PETs can protect corporate confidential information and protect revenues by securing the integrity of data.

1. Encryption. Encryption today is a relatively mature technology, though still in a state of advancement. Encryption supports the security and proportionality principles of data protection law. In the past two years we have seen an increasing trend for regulators to become more prescriptive in their approach to encryption, for example, in the PCI DSS standard for credit card data, and in a recent announcement by the UK data protection regulator. Encryption is relatively simple to implement and can be a highly effective tool.

2: Metadata and Digital Rights Management. Metadata and Digital Rights Management are far newer technologies than encryption. Metadata is data about data, providing a framework to describe semantics—the meaning of different types of data. Metadata can be very useful for achieving compliance with data protection legislation because one can differentiate between data, personal data and sensitive personal data. Certain data types such as religious information can be ‘tagged’ as being sensitive so that different rules of processing can be automatically triggered for example. More advanced applications of metadata revolve around uses of Digital Rights Management (DRM) applications. Originally intended to protect electronic copyright, DRM technology can be adapted to provide users with a very high level of control over how their personal information is used. When deployed on trusted infrastructure, it provides strong controllability, auditability and transparency (‘CAT’)—the privacy equivalent of information security confidentiality, integrity and availability (‘CIA’)—over the governance of personal information. These technologies tend to support in particular the purpose binding (controlling secondary use) and transparency (informing data subjects of their rights) principles of data protection law. Metadata schemes are relatively simple to implement for structured data sets and can be highly effective. Digital Rights Management technologies are less mature with implementation being more complicated. In terms of effectiveness however they offer significant support for privacy.

3: Application programming. Software packages processing personal data execute rules which determine how personal data is processed. It follows that those rules should uphold data protection regulatory requirements. When implicated rules are binary, for instance ‘opt-in’—‘opt-out’, as typically is the case with a permission management system, this is relatively straightforward, conceptually at least, and can be configured by the user organisation. Where rules are ‘fuzzy’, a term which can be used to describe evolving jurisprudence of privacy, the solution is more involved. Here, a given rule unlike a binary yes/no rule can effectively take on multiple different values given inherent imprecision. Embedding such ‘fuzzy’ rules into code requires a series of steps, translating given sets of jurisprudence into a formal logic, implementing that logic in a given programming language, and then verifying that that implementation maps to its logical instantiation through the use of formal methods. These activities are typically pursuant upon the software provider rather than the data controller.

4: System development governance. IT governance is a moderately mature area, and while many organisations include data protection controls in their system development lifecycle frameworks, those controls are often ‘checklist’ orientated. The inherent weakness with this approach is that to be effective, legal privacy risks need to be translated into language that makes sense to a IT professional, and controls to manage those risks need to be technologically prescriptive yet make sense to a lawyer. These two conditions are rarely met today. The result is that a large
amount of non compliance is designed into applications. Governance over system development can be a highly effective and efficient approach to supporting compliance.

5: User interface. Many professional user interface designers have only recently started to apply the discipline of ‘engineering psychology’ in their work. This applies principles of how the human mind constructs reality to the experience a user has of the two dimensional screen with which they interact. The primary legal requirement compelling the use of engineering psychology is that of the spirit of the transparency principle, primarily defined in Article 10 of Directive 95/E46/EC, the directive covering all personal processing in EU member states. Engineering psychology influences include font sizes, colours, sequencing of tasks, shapes, spatial movement and use of imagery. Data protection requirements, for a given situation (i.e. using a HR system, a CRM system, a social networking site), can be integrated into workflow through the use of engineering psychology. This strongly supports an individuals’ cognition of their rights.

6: Identity management. A fundamental principle of data protection is data minimisation. This can be applied to separate authorization (do you have the right to perform this action?) from identification (who are you?). Encryption can be selectively applied to partition access to particular categories or tables of personal data, keeping separate different identities users adopt for different spheres in their lives. This tends to empower people with the cryptographic property of ‘conditional linkability’, where users consent to any aggregation of their identities, with cryptography making it mathematically implausible to deduce one identity from another, in some contexts. Identity management tends to support the purpose binding (control over secondary uses), security and proportionality (restricting data usage) principles of data protection law.

7: Architecture. Architects can have a fundamental affect on data protection compliance. Design decisions on inbound and outbound system interfaces, use of cryptographic acceleration, database design, incorporation of anonymizer front-ends to Web servers and the application of trusted infrastructure are just a few situations where architectural choices can support privacy requirements and expectations. Architecture can become a PET strategy in itself as it has the potential to support all principles of data protection law.

“Driving an effective and efficient allocation of responsibilities for privacy requires the CIO to adopt an active custodianship role for data protection controls.”

Steve Kenny is KPMG’s Privacy Services Leader responsible for strategy definition and execution. Previously, he was appointed by Law to the European Commission to advise all EU member state data protection commissioners. Contact Steve at steve.kenny@kpmg.com.
Canadian Summit Overview

Canadian privacy pros gathered in Toronto May 21-23 for the first-ever IAPP Canadian Privacy Summit. Described as “outstanding,” “useful” and “memorable, the conference drew professionals and government officials from across the nation.

(Above) President of Holt Renfrew Caryn Lerner (left) and Canadian Retail Council president Diane Brisebois at the welcome reception

(Below) Assistant Privacy Commissioner of Canada Elizabeth Denham and B.C. Information and Privacy Commissioner David Loukadelis

(Above) Constantine Karbaliotis, Symantec’s Information Privacy Lead (left) and Antoine Aylwin, Associate at Fasken Martineau LLP, and co-chair of the “Outsourcing – A Privacy Dilemma” session.

(Right) Friday’s networking session on “Top Stay Awake Privacy Issues” was a popular favorite.
(Above) Lorne MacDougall, co-chair of the event and CPO at Holt Renfrew enjoys the opening night reception at Holt’s Café.

(Below) Ann Cavoukian and Facebook’s Chris Kelly at the Holt’s Café reception.

(Above) Four Canadian Information and Privacy Commissioners: (from left) Ann Cavoukian, Ontario; Frank Work, Alberta; Elizabeth Denham, Assistant Privacy Commissioner of Canada; and David Loukidelis, British Columbia.

(Above) Participants work in groups during Friday’s facilitated networking session on building privacy policy programs.

(Above) Co-chair of the event Terry McQuay, president of Nymity.

(Right) To top off a great week in Toronto, the Blue Jays kicked off a five-game winning streak, beating the Anaheim Angels 4-3.
CANADA

By Terry McQuay, CIPP, CIPP/C

Use of Generally Accepted Privacy Principles (GAPP) mandated by Information and Privacy Commissioner of Ontario

In a special investigation report, “Privacy and Video Surveillance in Mass Transit System,” published March 3, the Information and Privacy Commissioner of Ontario made several recommendations to the Toronto Transit Commission (TTC) regarding its deployment of video surveillance cameras. Prompting this investigation report was a complaint received from UK-based Privacy International relating to the use of video surveillance cameras throughout the city’s mass transit system. The report provides a comprehensive analysis of the use of video surveillance technologies in the areas of:
• notice;
• safeguards;
• retention periods;
• destruction processes; and
• training for employees.

To view the report visit www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf and to download the GAPP visit www.cica.ca/download.cfm?ci_id=36533&la_id=1&re_id=0

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.

FRANCE

By Pascale Gelly

Bad Grade for Grading Site

“Take the power, grade your teacher” is the claim of Internet site www.Note2be.com, which gave students the opportunity to grade their teachers and professors online. The site published the names of teachers or professors, the subject taught, the school or college where they practiced and the average grade given to them by Internet users, including a “Top 10” list.

The professors whose names appeared on the site initiated emergency judiciary proceedings on the basis of their rights to privacy and to the protection of personal data. As a result, the Paris criminal court ordered on March 3, 2008 the removal of the names of professors online.

In parallel, the French Data Protection Authority (CNIL), involved by trade unions, considered in an opinion on March 6 that this site did not meet the condition of legitimacy imposed on the processing of personal data by the data protection law for several reasons: 1) It could be mistaken for an official grading system. 2) Grading was too subjective and 3) its quality could not be verified and most of all, 4) the site owner had not obtained the prior consent of the concerned professors. Still, the site owners have announced that they will bring an appeal against the court decision on the ground of freedom of expression, as their
site lost great interest now that the names have been removed.

Guidance for online videogames

The “Forum des droits de l’Internet,” a recognized observatory of Internet practices, has published practical guidance intended for junior users of online video games, their parents and games publishers.

The guidance notes to the videogame industry address the main critical issues to be considered by game publishers: control of the users’ age; devices to sensitize users and their parents to the time spent online; the publisher’s obligations relating to the protection of personal data; rules applying to advertising within the game; liability for public or private messages posted on forums or sent by email messaging systems; and potential sanctions towards a user.

Law to Create Trust in Digital Economy

The Commission of Economic Affairs of the National Assembly is working on a report to analyze the impact of this Law of June 21, 2004. According to La Gazette du Net, a draft, not-yet-final, criticizing some court decisions (Tiscali, MySpace) would insist on maintaining the distinction between hosts and publishers. Indeed, hosts are subject to a limited liability regime under which they cannot be held liable for content unless they have been informed that their services are used to publish unlawful content and they have not deleted it promptly. The report would also call for a specific regime for auction sites, considering that the characterization of hosts is not entirely appropriate.

Who to notify of new performance evaluation system launch

AGME (Association pour la Gestion du Groupe Mornay Europe) employs 2,300 individuals and had planned to implement a project of performance evaluation based on interviews with employees. The employer presented the project to the works council, which objected that the project must also notify the CHSCT (Committee for Hygiene, Safety and Work Conditions) and to the CNIL (French Data Protection Authority). The social chamber of the Supreme Court confirmed on November 28, 2007 that the CHSCT had to be consulted before the implementation of this project, since the yearly evaluations were intended to improve consistency between salary decisions and the achievement of employees’ objectives. They could have an impact on the behavior of employees, their career evolution and their compensation, and therefore generate psychological pressure with consequences on employees’ work conditions. However, the Supreme Court upheld partly the decision of the Court of Appeal as it considered that since the individual interview form was on paper, the Court of Appeal had not evidenced that personal data would be subject to an automated data processing. Under the French Data Protection Act, non-automated processing does not have to be notified to the CNIL.

Cybermonitoring before Administrative Court

A frequent visitor of a public library has brought an appeal against a decision to temporary expel him for having used the Internet facilities of the library to access porn sites.

He claimed that he had not been given proper notice of controls of connections. The library’s internal regulation specified a clear prohibition to access porn sites and provided that the library’s staff was in charge of the implementation of these rules.

The administrative court of Pau considered that the provisions of the library’s internal regulation were sufficient to enable the library’s staff to operate controls of logs.

This decision seems to be less demanding in terms of notice than decisions in similar cases in an employment context which require a proper notice of data processing activities carried out in the framework of IT surveillance.

Pascale Gelly is Avocat à la Cour within SCM Lambot Gelly Soyer. She may be reached at pg@pascalegelly.com

“...provisions and target two issues long needed to be enacted.”

ISRAEL

Dan Or-Hof, CIPP

New bills would boost online privacy

Two new bills were recently introduced by the Israeli government: the Electronic Commerce Law and the Communications Law (Amendment No. 33). The two bills encompass privacy-enhancing provisions and target two issues long needed to be enacted—prohibition on spam and online anonymity.

Setting out to regulate certain legal aspects of commercial transactions in electronic media, the Electronic Commerce Law will impose a duty on online service providers to secure and keep confidential every detail and document that can personally identify the data subject. The law further instructs courts to order a person identity to be disclosed only upon showing a substantial likelihood that the person committed a tort or infringed on intellectual property rights.

The proposed amendment to the Communications Law adopts the EU ‘opt-in’ approach toward unsolicited commercial electronic messages. If approved, no such communications will be allowed through e-mail, fax, automatic dialing systems and SMS messages without prior explicit consent. Failure to comply will result in statutory damages of up NIS1,000 (approximately $285) per one unsolicited message and fines of up
Global Privacy Dispatches

continued from page 13

to NIS 202,000 (approximately $60,000).

Both bills were approved last February by the Israeli Parliament (the ‘Knesset’) in the first reading out of three, and are now under deliberations by the Knesset’s committees. It is expected that the bills will be enacted by the end of this year.

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.

UK

By Stewart Room

Information Commissioner suffers severe setback in data security campaign

The UK Information Commissioner has suffered a severe setback in his long-running campaign to see the introduction of custodial penalties for “data theft” contrary to section 55 of the Data Protection Act 1998. Earlier this month the UK Parliament suspended the operation of an amendment to section 55 that would have introduced custodial penalties, following highly effective lobbying by the UK press and media.

The background to this story is very interesting. In May 2006 the Information Commissioner used special powers in the Data Protection Act to submit a report to Parliament titled “What price privacy?” in which he said that he had uncovered evidence of a “widespread and pervasive” black market trading in stolen personal data. He identified private detectives as being at the heart of the black market. The essence of his case was that the current criminal regime for these offences—which focuses only on fines—is insufficient to deter criminal behaviour. Therefore, he submitted that custodial penalties need to be introduced. The following month the UK Government issued a consultation on these proposals, demonstrating that the Commissioner and the Government had acted in concert to some extent, and in early 2007 the Government announced that it would introduce the necessary amending legislation. This was eventually introduced within the Criminal Justice and Immigration Bill, in summer 2007.

However, in the period between “What price privacy?” and the government’s announcement that it would legislate, the commissioner published a follow-up report titled “What price privacy now?” (December 2006). This report marked the point when things started to go wrong for the Commissioner, because it “named and shamed” more than 30 leading UK press and media companies whom the commissioner said were involved in the black market. Not surprisingly, this incensed a considerable part of the press and media and the die was cast for a battle at the heart of Parliament, which the commissioner lost this month.

The state of play is that the Data Protection Act will be amended to give the government the power to introduce custodial penalties at a later stage. However, this compromise position looks to neutral commentators to be a challenge to the Commissioner: if he can stack-up the charges that he has made in his reports—in other words if he can secure convictions under the law as it presently stands—the Government might, just might, revisit the matter subsequently.


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.

By Michael Spadea, CIPP

UK Financial Services Firm Signs ICO Undertaking

Skipton Financial Services has signed an undertaking requiring it to encrypt personal data stored on laptops after a laptop containing the financial details of 14,000 customers was stolen from a contractor. The laptop contained names, dates of birth, national insurance numbers and investment amounts. This is the latest Information Commissioner Office (ICO) action pushing encryption of personal data on laptops. Businesses under ICO jurisdiction should require service providers to encrypt personal data stored on laptop computers and also, perhaps, on all portable storage devices. Relevant language should be either in the body of the agreement or in the attached security schedule.

London Police Regularly Access Public Transport Records

In the past year, London Police have made more than 3,000 requests for passenger journey details on London public transportation. Passengers who use the Oyster card, a contactless smartcard, have their trip data stored for two months. Passengers who register their cards with Transport for London to protect against theft have their personal information linked with their trip details. The concern is that transit users are not
informed that their data may be shared with the police or that their data is retained for two months. Transport for London states that the ICO is familiar with the details of the Oyster card system and has not expressed any concern.

**NHS Laptop Containing Sexual and Physical Abuse Histories Stolen**

Over the past five years, nearly 200 electronic devices from Lothian public bodies (a region in Scotland) have gone missing. One such device contained the psychiatric and personal history of a person who had been physically and sexually abused. That device, a laptop, was stolen from a consultant in October 2005, but is only now being made public. Edinburgh University, where the study was being conducted, stated that the data was wrongly downloaded, but that they have since changed their policies to prevent a recurrence.

**Terminal 5: Business v. Security**

The British Airport Authority is under fire from the ICO for its decision to use fingerprints to log entry and exit to the departure lounge. The BAA’s business model is to allow all passengers, whether international or domestic travellers, to access the shops and restaurants in Terminal 5. The physical configuration that allows this has created a security vulnerability: an individual seeking to enter the country illegally could swap tickets in the lounge and slip into the UK via a regional airport without going through immigration. The same configuration exists at Gatwick airport, but instead of fingerprinting, a photo is taken and a barcode is attached to the boarding pass. The ICO is concerned that fingerprinting is too intrusive and has requested additional information. Both the BAA and the government blame each other for the problem and the solution.

Michael Spadea is a London-based privacy attorney. He may be reached at mspadea@gmail.com, or at +44 (077) 80624543.

---

**New Faces at the IAPP**

**The IAPP is pleased to welcome Wills Catling.**

**Wills Catling**

**Sales Director**

Wills Catling joined the IAPP in February as sales director. He is responsible for the growth and retention of membership; sponsorship and exhibit opportunities for the IAPP’s annual events; and advertising opportunities in IAPP publications.

Wills comes to us with 14+ years of sales experience in the financial and mortgage industries, as well as eight years working for the second largest insurance company in his native UK, Norwich Union.

---

**The Lighter Side of Privacy**

GET ALL THE INFORMATION YOU CAN, WE’LL THINK OF A USE FOR IT LATER.

Reprinted with permission from Slane Cartoons Limited.
Congratulations, Certified Professionals!

The IAPP is pleased to announce the latest graduates of our privacy certification programs. The following individuals successfully completed the CIPP examinations held in March and April 2008:

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/CRP 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!
Every major data protection law or regulation requires organizations to have a written information protection plan!

The Federal Trade Commission and other regulatory enforcement agencies have cited the lack of written policies in assessing recent fines for violations of data destruction requirements.

The NAID Information Destruction Policy Compliance Toolkit, created by security, legal and information management professionals, provides the easiest, most comprehensive system for developing written information destruction policies and procedures to meet regulatory requirements and protect your organization.

The NAID Information Destruction Policy Compliance Toolkit is available through any authorized NAID Member. To find a NAID Member near you, go to www.naidonline.org and click on the “Compliance Toolkit” banner.
Privacy expert joins Proskauer Rose LLP

Kristen Mathews joins New York firm

IAPP member Kristen Mathews, CIPP, has joined Proskauer Rose LLP’s New York office. Mathews specializes in technology, e-commerce and media-related transactions and advice, with concentrations in the areas of data privacy, data security, direct marketing and online advertising. Mathews is part of Proskauer’s Privacy and Data Security and Technology, Media & Communications Practice Groups. She advises clients on responding to data security breaches, preparing privacy and data security policies, payment card data security and other technology areas.

Before Proskauer, Mathews was a partner at Thelen Reid Brown Raysman and Steiner LLP, where she headed Thelen’s Privacy and Data Security Practice Group.

Don’t Mess with Texans’ Identities

As part of an ongoing effort to prevent identity theft in the state, the Texas Attorney General has launched a Web site to help citizens avoid becoming victims of what has become the fastest growing white-collar crime in the nation. Texas ranks second in the nation for the number of ID theft complaints.

The site includes tips for prevention as well as an Identity Theft Victim’s Kit that victims can use to minimize damage, and a video that features testimonials of actual identity theft victims. www.texasfightsidtheft.gov

Siemens CPO Re-Elected to HITSP

Donald Bechtel, chief privacy officer of Siemens’ Healthcare Data Exchange, was re-elected to the Board of Directors of the Healthcare Information Technology Standards Panel (HITSP). Bechtel is currently serving his second term as co-chairperson of the Healthcare Task Force Group, which develops and maintains the financial and administrative healthcare transactions used by the insurance industry for the Health Insurance Portability and Accountability Act (HIPAA) and other purposes.

Australia Launches Privacy Awards

Nomination Deadline 9 July

The Australian Privacy Commissioner is accepting nominations for the inaugural Australian Privacy Awards and Australian Privacy Medal. The awards aim to recognise businesses, government agencies and nonprofit organizations who have demonstrated an outstanding commitment in the field of privacy. The Privacy Medal will acknowledge an individual who has gone above and beyond in advancing privacy in Australia. Winners will be announced at a gala event in August.
Alterian Names Vice President of Deliverability and Privacy

IAPP member David Fowler has joined Chicago-based enterprise marketing platform provider Alterian as that company’s Vice President of Deliverability and Privacy. Formerly, Fowler served as Global Vice President of Deliverability & Privacy Services at BlueHornet.

Data Security Event

Privacy and legal professionals from various disciplines gathered in Chicago on April 15 for a free one day workshop on “Protecting Personal Information: Best Practices for Business.” From left: John Jensen, CIPP, Officer of the Senior VP for Health Services at the University of Minnesota’s Academic Health Center, Justine Gottshall, CIPP, of Wildman Harrold, and Judy Macior, CIPP/G, CIPP/C, of Experian. The event was sponsored in part by the Federal Trade Commission.

SUNERA

Rise above with SUNERA’s data privacy consulting services:

- Privacy Risk Assessments
- Policy Development
- Breach Notification Procedures
- Safe Harbor & EU DPA Registrations
- Awareness Training
- PCI Compliance

Visit our booth at the IAPP Privacy Summit 2008 to receive a comprehensive summary of the privacy protection requirements of domestic and international data privacy legislation. We will also be demonstrating our Open GRC suite which automates privacy compliance monitoring. For more information about Sunera and our services, visit us at www.sunera.com.
Calendar of Events

JUNE

4 IAPP/CIS Webinar — Coordinating Privacy and Infosecurity for Effective Data Protection
   11 a.m. - 3 p.m.
   Speakers: Peggy Eisenhauer, CIPP; guest speakers.
   Up to 3.5 CPE credit hours for eligible CIPPs

10 IAPP KnowledgeNet — Charlotte, NC
   Tuesday, June 10, 2008
   11:30 a.m. – 1 p.m.
   Speaker: Mike Guiterman, Director of Compliance Product Management at Sourcefire
   Topic: "You're Compliant but Are You Secure?"

16-17 Practical Privacy Series — New York, N.Y.
   The Graduate Center, CUNY

17 IAPP Certification Testing — New York, NY
   CIPP, CIPP/G and CIPP/C examinations
   5 – 8:30 p.m.
   IAPP Practical Privacy Series
   The Graduate Center, City University of New York (CUNY)
   365 Fifth Avenue
   New York, NY

20 IAPP Certification Testing — San Francisco, CA
   CIPP, CIPP/G and CIPP/C examinations
   1:30 – 5 p.m.
   Ernst & Young
   560 Mission Street
   Training Room
   San Francisco, CA 94105

21 IAPP Certification Testing — Richmond, VA
   CIPP, CIPP/G and CIPP/C examinations
   9 a.m. – 5 p.m. EDT
   Capital One Campus
   15000 Capital One Drive
   Richmond, VA  23238

30 IAPP Certification Testing — Washington, D.C.
   CIPP, CIPP/G and CIPP/C examinations
   1 – 5 p.m.
   Ernst & Young
   1101 New York Avenue, NW
   Room 3.1069 J&K
   Washington, D.C. 20005

JULY

24 The Town Hall
   The Federal Trade Commission and the Technology Law and Public Policy Clinic, University of Washington School of Law
   William H. Gates Hall, Room 133
   15th Avenue NE & NE 43rd Street, Seattle, WA

SEPTEMBER

22-24 IAPP Privacy Academy 2008 — Orlando, Fla.

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