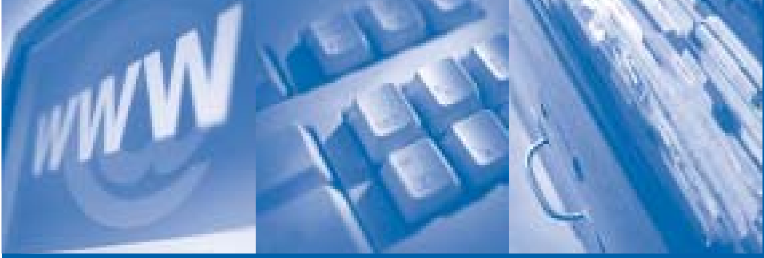


INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

India gives commitment on new privacy initiative

India's government gave a commitment on September 30th last year to introduce a data protection initiative for companies outsourcing their data processing operations. But which type of proposal is the government most likely to adopt? **Stewart Dresner** reports from New Delhi.

Following the parliamentary election in April, the new government is likely to press ahead with data protection proposals directed at companies in India, often with headquarters in Western Europe or North America carrying out business process outsourcing, such as IT contracts and customer call centres.

The Indian government finds itself caught between a wish to satisfy its largest trading partner, the European Union, encouraging a law based on the model of the EU's Data Protection Directive, and US-based companies which would prefer a contractual approach and see no need for legislation.

> India wishes to tread carefully and not introduce any bill which is likely to alienate American business opinion.

The EU approach

The EU's approach was emphasised by the European Commissioner for Information Society, Erkki Liikanen, at the EuroIndia 2004 Cooperation Forum on the Information Society, held in New Delhi, March 24-26th. Data protection and information security issues were addressed on the first day and Liikanen also discussed data protection with Arun Shourie, Minister for Disinvestment, Communication and IT.

At stake is the ability of the companies carrying out work outsourced to them to manage the personal data in their care in a way which maintains its security, and to respond in a timely way to any requests by individuals for access to and correction of their personal data, or fulfilment of any of their other rights.

The US approach

The approach from US industry is that there is no need for an Indian law because all the issues surrounding the processing of personal data can be handled by contracts between an organisation's US headquarters and the data processing company based in India. For example, the global privacy manager for a major US-based IT systems company told *PL&B International* that a European-style privacy law in India would simply add to compliance costs and give no material benefit to individuals which they did not already enjoy as a result of contracts which his company and others already had in place.

Continued on p.3

Issue 72 **March/April 2004**

NEWS & ANALYSIS

REGULATION

MANAGEMENT

INTERNATIONAL newsletter

ISSUE NO 72 March/April 2004

EDITOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

ASSOCIATE EDITOR
Eugene Oscapella
eugene@privacylaws.com

NEWS EDITOR
Alan Pedersen
alan@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 72 CONTRIBUTORS
Jim Runsten
Bird & Bird

Laura Linkomies
Privacy Laws & Business

Lilly Taranto
Marketing Improvement

James Michael
Universities of London and Cape Town

Walter Janowski
Gartner

PUBLISHED BY
Privacy Laws & Business,
5th Floor, Raebarn House,
100 Northolt Road, Harrow,
Middlesex, HA2 0BX,
United Kingdom
Tel: +44 (0)20 8423 1300,
Fax: +44 (0)20 8423 4536
Website: www.privacylaws.com

Design by ProCreative +44 (0)20 8429 2400
Printed by Direct Image +44 (0)20 7336 7300

ISSN 0953-6795

“comment”

India at the data protection crossroads

India, whose citizens comprise one of the world’s oldest and culturally rich societies, is now confronting a very modern cultural issue, as Stewart Dresner reports in this issue of *PL&B International*.

India has shown little interest in enacting data protection legislation as a vehicle to protect the privacy rights of Indians, since this appears to be a much lesser priority than other more pressing social issues. And what little pressure there is to enact such legislation encounters the real concern that India will become less attractive as a place for US companies to outsource their activities if data protection measures alienate American politicians and businesses. Already in this US election year, politicians and businesses are becoming skittish about outsourcing. Restrictive data protection laws may provide the excuse that they need to discourage outsourcing. The result for India could be the serious weakening of a vital technological and economic driver.

On the other hand, EU countries may be reluctant to outsource to India unless they are assured an adequate level of protection for any personal data that is transferred to India.

The Indian government therefore finds itself caught between a wish to satisfy its largest trading partner, the European Union, and US-based companies that have shown a marked preference for a contractual approach without data protection legislation. As Stewart Dresner’s article shows, India must now engage in a delicate balancing act as it faces a range of options for reconciling data protection concerns with important business imperatives. *PL&B International* will continue to watch how the world’s second most populous country will respond in the coming months and years.

Eugene Oscapella, Associate Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B Newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Alan Pedersen on Tel: +44 208 423 1300, or E-mail: alan@privacylaws.com.

India commits to data protection, continued from p.1

OUTSOURCING IS INDIA'S DATA PROTECTION DRIVER

This analysis is confined to the outsourcing context because there is little pressure from Indian human rights groups for a law for protecting the privacy rights of Indians, explains Anindya Acharya, Deputy Director of IT at the Confederation of Indian Industry (CII). The reason is that for India-based human rights groups, computerisation of Indian society has not developed to the extent where there is a substantial awareness of privacy. Other issues, such as the status of women, community health and educ-tion, are a much higher priority.

There are also other much more pressing issues for India-based businesses. The CII announced on March 30th that its new agenda will focus on environment-friendly business practices and lobbying for cleaner technology to minimise pollution, better communication and connectivity, adequate power supply, availability of water and more investment into infrastructure.

This does not mean that business has been silent when there were proposals for data protection laws over the last two years, according to Pavan Duggal, head of India's leading niche cyberlaw firm, Pavan Duggal Associates, and Advocate at the Supreme Court of India. Duggal told *PL&B International* that when in 2002 the government of south-eastern state, Andhra Pradesh (AP), proposed a data protection bill based closely on the EU Data Protection Directive, the companies consulted opposed the bill. They argued that it would increase compliance costs both for companies established in the state and those considering investing in business process outsourcing there. The AP government therefore reconsidered and before submitting the bill to the state legislature for debate, put the bill on hold, sensitive to companies' arguments that it was essential to protect their investment and jobs in AP.

It was considered that an AP data protection law would reduce the attractiveness of the state as a location for inward investment if there were a legal environment inconsistent with other states which were equally interested in receiving a slice of the growing foreign investment in business process outsourcing.

Duggal explained that although India's constitution permits the states to legislate on special contracts - which is why AP's bill was described as a "special contracts" data protection bill – the federal Ministry of IT decided to take the initiative on legislating a data protection regime. The ministry decided that it was unwise to project internationally an image of India as a country which was not a secure location for processing personal data.

As a result, later in 2002, India's National Association of Software and Service Companies (NASSCOM) published its own bill which represented a middle way between doing nothing and adopting a comprehensive EU-style data protection law. Soon afterwards, the IT Ministry established an advisory committee of three lawyers, including Pavan Duggal.

the European Commission shows little sign of wanting to repeat the lengthy negotiations which were needed to secure a safe harbor agreement with the US

PRIVACY AS A POLITICAL ISSUE

Data protection is not an issue in the run-up to the April parliamentary elections. None of the political parties have so far made a statement on the subject but they have spoken on the need for an enabling environment for outsourcing.

However, one factor complicating the issue is that there is currently a groundswell of opinion in the US against outsourcing. Presidential candidate, John Kerry, has spoken of the loss of jobs from the US resulting from outsourcing to countries such as India. In such a climate, India wishes to tread carefully and not introduce any bill which is likely to alienate American business opinion.

Job losses and data security fears have also been raised in the UK. British members of the European Parliament have been lobbying for an EU investigation into outsourcing to India. They are calling for strong data protection safeguards and a requirement that will force companies operating in India to inform customers where they are calling from.

THE POLICY OPTIONS

There are broadly six policy options facing the IT Ministry's Advisory Committee:

1. Do nothing - This would be an easy option as India has attracted a significant inward investment in outsourcing with no data protection law. Companies deal with data protection law issues, if they wish, by leaving it to contracts between company headquarters and the data processing companies in India. This option appears attractive to US-based business.

2. Publish data protection guidelines - This option has the merit that it provides the government with the sense that it is fulfiling its September 2003 commitment to take action on data protection without imposing legally binding and costly obligations. The data protection guidelines could be on the lines of the EU's data quality principles or Canada's fair information practices. The CII hopes that such guidelines will be published later this year.

3. Negotiate an Indian Safe Harbor - From India's perspective, negotiating a Safe Harbor Agreement with the European Commission has certain attractions and this option is favoured by the CII and NASSCOM. It would give Indian companies an opportunity to declare to an Indian government agency that they were fulfiling many of the requirements of the EU Data Protection Directive in their own way. That declaration would then give these India-based companies an adequacy status without the time consuming effort of adopting a national data protection law. However, the European Commission shows little sign of wanting to repeat the lengthy negotiations which were needed to secure a safe harbor agreement with the US.

The CII's Anindya Acharya argues that India does more business with the

Continued on p.17

global privacy roundup

AUSTRALIA

On April 11th, the Federal Spam Act came into force. The law includes all forms of electronic marketing and covers advertising sent from overseas. Electronic marketing can not be sent without express consent from consumers, unless there is an existing business relationship. All messages must also identify the sender and provide an opt-out facility.

Penalties for breaching the Act include fines of up to AUS$220,000 (€137,000) per day and up to AUS$1.1 million (€685,000) for repeat offenders. Basic guidance published by the Australian Communications Authority can be found at www.aca.gov.au.

EUROPEAN UNION

In April, the EU Data Protection Working Party published its agenda for 2004. Issues to be addressed include developments on the Binding Corporate Rules scheme for international data transfers, simplifying notification procedures, more effective enforcement mechanisms, and working towards an assessment of the privacy laws in Australia and New Zealand.

Additionally, the Working Party has published a number of sector-specific reports including electronic marketing (see p.10), video surveillance, and genetic data.

GERMANY

The German Parliament passed new regulations on unsolicited e-marketing and spam in April. The Law Against Unfair Competition transposes the Privacy & Electronic Communications Directive which was passed in 2002.

The original deadline for implementing the directive was October 2003 and Germany's slow response led to a second warning from the European Commission in early April (see p.7).

HONG KONG

Privacy Commissioner, Raymond Tang, has published guidance for organisations that share marketing data with third parties.

The guidance looks at how personal data should be handled when conducting joint marketing campaigns, recommending that customers be informed about third party advertising prior to any marketing material being sent out, or when their details were first collected.

An organisation handing customer data over to partners should either ensure that it is limited to what is strictly necessary and not used for other purposes, or consider host mailings as a less intrusive alternative. For more information see www.pco.org.hk

IRELAND

In April, the data protection commissioner, Joe Meade, delivered his first annual report under Ireland's new data protection law, which came into effect in July 2003.

The report highlights a sharp rise in complaints with investigations carried out by the commissioner's office revealing a number of compliance issues, including marketing to minors and SMS spam, recruitment and HR, and the disclosure of medical data. Most complaints to the commissioner's office were resolved informally although two law firms were prosecuted for failing to register with the data protection authority.

ITALY

At the end of February, the Italian Data Protection Authority (Garante) warned that organisations will not be allowed to use information from electoral roll lists when conducting marketing campaigns via SMS, mobile phones or e-mail. Under Italy's new Data Protection Code, which came into force on January 1st 2004, marketers are required to obtain explicit opt-in consent from consumers when carrying out electronic marketing campaigns. However, organisations will still be able to use electoral roll data to send out postal advertising, or even contact consumers by telephone - provided that they are given adequate information notices and the calls are not made by automated dialing systems.

JAPAN

On April 2nd, Japan's government approved a set of 'basic' privacy guidelines. The guidelines aim to complement Japan's Personal Information Protection Law, which was passed in May 2003. The guidelines will apply to all private and public sector organisations that hold data on 5,000 or more individuals, and will require organisations to appoint representatives with responsibility for privacy compliance, as well as developing procedures to prevent unauthorised access to personal data. The guidelines also envisage the creation of further sector-specific guidelines (on areas such as telecommunications, healthcare and financial services) which will be regulated by the relevant government ministries.

Privacy & American Business has launched a new service which aims to help multinationals address privacy issues in their Japanese operations. The service provides users with details on Japan's privacy law and regulations, access to case law, consumer research, and examples of corporate privacy policies. For more information: www.privacyexchange.org

MALAYSIA

In March, the Malaysian government suggested there could be further delays to the introduction of the Personal Data Protection Act. According to Malaysian news service, *The Star*, government minister Dr Rais Yatim said that the delay was due to the need for further comparative studies to ensure that international data protection standards are met.

Although the bill was due to be discussed by Parliament in March, it could now be delayed until the next sitting later this year.

SWEDEN

Sweden's new regulations on electronic marketing came into effect on April 1st. Businesses marketing to Swedish citizens will now have to obtain explicit (opt-in) consent before sending them advertising via e-mail, SMS or fax. See p.10 for full report.

UNITED KINGDOM

UK members of the European Parliament (MEPs) have been lobbying for stronger safeguards for personal data outsourced to third parties outside the EU. At the beginning of April, the MEPs called for stronger enforcement of European data protection laws and a requirement for companies operating outside the EU to inform customers from where they are calling.

The Department of Trade & Industry has confirmed that the government will introduce a new telemarketing registry for business users on June 25th this year. Businesses will be able to opt-out from receiving telemarketing calls by registering their phone numbers onto a national do-not-call list.

UNITED STATES

In March, two US senators introduced a bill aimed at restricting the commercial exchange of data on children. The proposed Children's Listbroker Privacy Act would place a ban on the sale of personal data relating to anyone under 16, unless parental consent has been obtained. The bill goes further than the existing Children's Online Privacy Protection Act (COPPA) which currently applies only to children under the age of 13.

Meanwhile, at the end of February, the Federal Trade Commission announced major settlements with two companies for allegedly infringing COPPA by collecting data on under 13s without parental consent. UMG Recordings agreed to pay a $400,000 civil penalty, while Bonzi Software agreed to pay $75,000.

16 events diary

Advanced Legal Data Protection & Privacy Forum
May 19-20, London, UK
Providing case studies and legal advice on issues such e-marketing, data transfers and subject access requests, this conference features speakers from the Information Commissioner's office, the European Commission and leading UK businesses.
Contact: Centaur Conferences
Tel: +44 (0) 207 970 4770
E-mail: conferences@centaur.co.uk
Website: www.centaur-conferences.co.uk

5th National Global HR Privacy Conference 2004
May 26-27, Washington, United States
Featuring presentations on issues such as outsourcing, data transfers, medical privacy and employee monitoring. The conference also features international updates on countries such as Germany, the UK, Canada, Hong Kong and Japan.
Contact: Privacy & American Business
Tel: +1 201 996 1154
Website: www.pandab.org

IAPP - TRUSTe Symposium: Privacy Futures
June 9-11, San Francisco, United States
Examining the privacy developments and future challenges for commercial business, this event focuses on how privacy affects corporate brands, privacy ROI, the role of technology and more.
Contact: Shara Prybutok, IAPP
Tel: +1 (800) 546 3750
E-mail: shara.prybutok@privacyassociation.org
Website: www.privacyfutures.org

Privacy Laws & Business' 17th Annual International Conference
July 5-7, Cambridge, UK
The focus of this year's conference is how to integrate privacy into your business strategy. 50 speakers including regulatory authorities, privacy managers and industry groups will address key issues such as outsourcing, marketing and HR.

A full programme will be available shortly via our website. See: www.privacylaws.com/whats-newframe.htm

How to use the Information Commissioner's DP Audit Manual
May 10-11, 2004 - London; July 6-7, 2004 - Cambridge
Privacy Laws & Business is conducting a series of interactive audit workshops across the UK or available in-house.
Contact: Glenn Daif-Burns, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
E-mail: glenn@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

The Data Protection Act Explained - Basic Training for Beginners
April 27 - Manchester; June 9 - London; September 21 - London; October 26 - Glasgow; December 7 - London
Privacy Laws & Business consultant, Valerie Taylor, presents a series of training workshops aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act.
Contact: Glenn Daif-Burns, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
E-mail: glenn@privacylaws.com

Privacy groups attack Google Gmail

Google has landed itself in hot water with the pro-privacy lobby over plans to introduce a free e-mail service for web users.

Over the last few years, Google has outstripped its competitors to create the world's most popular search engine and it now aims to repeat that success by taking on the likes of Microsoft and Yahoo! in the web-based e-mail space.

The selling point for the new 'Gmail' service, aside from being free, is that users will be given a massive 1 gigabyte storage space. But nothing, of course, comes for free and it seems that the price consumers will have to pay is their privacy. Google's Gmail service will aim to generate revenue by scanning users' e-mail accounts and then delivering targeted advertising based on the contents of the messages.

Concerns have also been raised over Gmail's privacy policy which states that "residual" copies of e-mails may remain on Google's systems even after users have terminated their accounts.

Privacy International has already filed complaints in 17 countries, while officials at Germany's federal data protection authority have voiced concerns over Gmail's compatibility with its privacy law. In the US, a coalition of privacy groups has written an open letter of complaint to Google executives, and Californian senator Liz Figueroa recently announced she is considering legislative action to tackle the privacy issues.

Such has been the public furore over Gmail that Google is reportedly mulling over changes to the service, including the possibility of allowing users to opt-out from receiving advertising. The official word from Google, however, is that the service is still at the testing stage and it is not going to jump into any "rash" decisions.

As to the debate on whether Gmail actually violates any national privacy laws, arguments are still being put forward on both sides. Nethertheless, Google has been dealt a blow in the publicity stakes - a simple lookup on its own search engine makes it painfully clear just how much adverse attention it is receiving.

US study reveals privacy spending trends

A new study carried out by the Ponemon Institute has revealed how US-based multinationals are budgeting for their privacy compliance programmes. Results from the IBM-backed *Cost of Privacy* study have shown that while privacy is becoming a higher priority, it is still taking a back seat to other regulatory obligations. 95 per cent of the 44 respondents to the survey felt that their organisations spent less on privacy than on compliance with environmental regulations.

The study showed that organisations with a more mature privacy compliance setup tend to spend more than those in the early stages. The multinationals studied fell mainly into three categories: (1) the planning/architecture stage (spending an average of $3.9 million), (2) the launch and implementation stage (an average of $6 million), and (3) the operational and ongoing maintenance stage (an average of $14 million).

The study found that organisations in the later stages of their privacy compliance programme require higher budgets in order to carry out privacy audits, implement employee training programmes, obtain website certification and privacy seals, and ensure third party processors meet their legal and contractual obligations.

Interestingly, the study found that technology companies spend the most money on privacy compliance, as opposed to the more heavily regulated sectors such as finance and healthcare services. Transportation and the hospitality industries spend the least on privacy initiatives.

In terms of the budgets allocated to privacy enabling technologies (PETs), the survey found that only ten per cent of companies were using PETs to enhance compliance or mitigate business risks. According to Steven Adler, marketing manager for privacy and compliance at IBM Tivoli, this is because adoption of privacy technologies is still in its early stages. "In general, privacy management is moving from legal policy to an operational IT domain, just like other regulatory compliance issues," he said. "Chief information officers today are just as concerned about building privacy management into IT infrastructure as chief privacy officers are about building effective human policies and training."

The kinds of technology that companies will adopt are likely to fall across a range of privacy compliance areas, from managing marketing and privacy preferences, through to digitising privacy policies and automating internal compliance procedures.

The rise in identity theft, data spillage as a result of viruses and worms as well as the huge problems caused by spam is costing industry dearly. According to Adler, privacy and security-related incidents last year cost the global economy $250 billion in direct damages and lost productivity, providing a huge incentive for organisations to implement robust compliance controls. "The only way to control further damage from these problems is to stem the flow of private information into the public domain, and to do so requires IT investment in privacy technologies to embed sound data management and disclosure control into the IT systems that collect and disseminate that information."

European Parliament wants more say over data transfers

A resolution adopted by the European Parliament in March, has criticised the way in which the EU handles international data transfers and has called for more say in the decision making process.

The resolution focuses on the European Commission's report on the implementation of the EU Data Protection, which was published in May last year.

The Parliament lambasted disparities in the way EU countries' handle data transfers, describing some approaches as "excessively rigid" while others as far too "permissive". It also suggested that the disparity is not only affecting data transfers outside Europe, but also internal data flows within the EU. The Parliament said that the "free movement of personal data is vital for the smooth operation of virtually all Union-wide economic activities; it is therefore necessary to resolve these differences of interpretation as soon as possible, to enable multinational organisations to frame pan-European data protection policies."

While the Parliament broadly supports the European Commission's view that the directive should not be changed, it has called for an amendment regarding the process for assessing whether so-called "third" countries meet the EU's data protection standards. It now wants the power to approve the Commission's "adequacy" decisions.

The proposal reflects the ongoing conflict between the Parliament and European Commission over the transfer of airline passenger details to US authorities. The Parliament has been extremely critical of the Commission's attempt to broker a deal with the US, branding it illegal and threatening to take the issue to the European Court of Justice.

Overall, the Parliament's resolution does provide some reassurance for the business community, accepting that organisations need to be able to operate in a "less complex and burdensome environment". It wants to see unnecessary legal obstacles removed and more choices for exporting data to be made available.

Additionally it has also recognised the value of self-regulation as opposed to excessively detailed legislation and has called for the business community to develop a European code of conduct.

EU issues 2nd warning over spam directive

The European Commission is continuing its pressure on EU countries that have failed to transpose the Privacy & Electronic Communications Directive into national law.

Last November, the Commission issued an initial warning to nine countries including Belgium, Germany, Greece, Finland, France, Luxembourg, the Netherlands, Portugal and Sweden. Since then, only Sweden and Germany have taken the appropriate action (see p.10).

The Commission has now delivered a second warning, sending what it refers to as "reasoned warnings" to the remaining countries. They now have until June to provide a reasonable explanation for not transposing the directive. Failing to respond could lead to prosecution by the European Court of Justice.

Framework on short privacy notices launched in Berlin

A group of 23 companies, privacy regulators and consumer organisations from Europe, North America and Australia met in Berlin on March 23rd and agreed on a framework for providing short privacy notices to consumers.

The meeting was convened by Richard Thomas, UK Information Commissioner; Dr Alexander Dix, Data Protection Commissioner, Brandenburg, Germany; Malcolm Crompton, Privacy Commissioner, Australia; and Martin Abrams, Executive Director, Centre for Information Policy Leadership, US. It followed a resolution on short notices adopted at the Privacy Commissioners' Conference in Sydney last September.

The aim of the meeting was to find a solution for improving the presentation of privacy notices, which tend to be overly long, complex, and cluttered with legal jargon. Although many notices are legally correct, the complexity can cause consumer resentment and make them wary of organisations' data handling practices. From the perspective of privacy regulators, complex notices frustrate their aims of raising consumer awareness and improving compliance with data protection laws.

The agreed framework states that short privacy notices should:

- refer to where more detailed information may be easily found
- contain language that the target group can easily understand
- be part of an information package that complies with relevant laws
- follow a consistent format and layout to increase consumer familiarity and understanding; and
- contain an essential minimum level of information.

Richard Thomas and Martin Abrams will speak on short privacy notices at PL&B's 17th Annual International Conference in July (see the events diary on p.5 for more details).

GMAC laptop theft highlights gaps in offsite security

GMAC Financial Services were at the centre of a serious privacy incident last month after compromising around 200,000 customer accounts. **Alan Pedersen** asks whether better security practices could have avoided embarrassment.

In March, an employee at GMAC, the credit lending arm of General Motors, had two laptops stolen from the locked boot of their car. According to *Information Week*, which broke the story, details on around 200,000 customers were stored on the laptops, containing a veritable treasure trove of information for ID fraudsters - names, addresses, dates of birth, social security numbers, and credit scores.

Stolen laptops are, of course, an inevitable risk for companies keen to promote flexibility and mobility in their workforce. Replacing stolen hardware is an inconvenience, but compromising the customer data stored on hard drives can have huge implications for a company's reputation - especially one that operates in the financial services sector. In GMAC's case, it appears there was a major failing in security. A spokesperson for the company told *Information Week* that although the laptops were password-protected, no encryption was used.

Replacing stolen hardware is an inconvenience, but compromising the customer data stored on hard drives can have huge implications for a company's reputation.

As a result, GMAC was forced into sending out letters to affected customers warning that their details may have been compromised and recommending they place a fraud alert on their credit files. The spokesperson said that the company would be reviewing its security policies and was now prohibiting employees from storing 'certain' information on laptops.

The fact that the laptops were only password-protected is somewhat surprising and bucks the trend among financial services companies, which traditionally tend to be more security-savvy than those in other sectors.

Experts agree that if you are taking valuable data outside the bricks and mortar safety of the office environment, you are going to need something a little stronger than a password. Protecting information on your laptop with a password is about as safe as, well, locking it in the boot of your car.

ASSESSING THE RISK

Yag Kanani, partner in charge of information security services at Deloitte & Touche, said that remote security policies should be based around a risk assessment framework. "Companies need to look at what the risks are and what the business impact would be if that data fell into the wrong hands," he said.

For customer data stored remotely on laptops or PDAs, Kanani said encryption is the best practice approach, although the overheads involved can put companies off. "A lot of organisations instead tell their users not to store sensitive files on their laptops, rather than encrypting files." But the problem with this kind of policy, he explained, is that a lack of awareness or just straightforward refusal to follow the rules can create gaps in compliance. "Awareness is a big issue, I seldom see good awareness programmes within organisations," he explained. "Even if you do these things at an optimum standard, you still have to protect against a disaffected employee who might try to steal data."

ENCRYPTION

Andrew Beard, advisory services director at PricewaterhouseCoopers, said that businesses are using different methods to encrypt customer data. "In many cases, organisations are taking the approach that everything is encrypted by default. There are other methods that allow you to create virtual drives and just encrypt the data on those drives." The latter option, he said, enables better performance for laptops, but there is a trade-off on security in that all data is not automatically encrypted. "The downside is obviously that as an organisation, you're passing control to your users and relying upon them to make that decision."

DON'T GET COMPLACENT

All large organisations handling customer data will have security policies and procedures in place. But perhaps the GMAC incident serves as useful warning that companies should not be sitting back too comfortably. While compliance gaps can easily occur, the security breaches that may arise as a result are not so easy to clean up.

ISPs win file-sharing privacy case

Eugene Oscapella reports on how Internet service providers (ISPs) are successfully playing the privacy card in an attempt to avoid disclosing the identities of customers engaged in online file-sharing of copyrighted music.

A March 31st decision of Canada's Federal Court has stressed privacy concerns in refusing to order several ISPs to disclose the identity of 29 customers who allegedly infringed copyright laws by illegally sharing music files online.

The plaintiffs, a coalition of major Canadian record labels, had wanted the names to enable them to sue individuals it claimed were frequent online music sharers. The record labels said they were unable to determine the name, address or telephone number of the Internet users, as the file sharing software they were using allowed them to operate under pseudonyms.

Customers' expectation of privacy was based on both the terms of their account agreements with the ISPs and with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA).

All of the parties to the motion agreed that ISP account holders have an expectation that their identity will be kept private and confidential. Customers' expectation of privacy was based on both the terms of their account agreements with the ISPs and with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA). They also agreed that PIPEDA allows ISPs to disclose personal information without consent under a court order.

The Court rejected the application for an order to disclose for several reasons, among them that downloading a song for personal use does not amount to a copyright infringement under current Canadian law (in early April, the federal government announced its intention to draft an amendment to outlaw such downloading). However, the Court gave several justifications relating to data quality and processing for its refusal to grant the order:

- There was no evidence explaining how a pseudonym was linked to a given IP address. It would be irresponsible for the Court to order the disclosure of the name of the account holder of that IP address and expose this individual to a lawsuit by the plaintiffs.

- The information being sought was not routinely kept by the ISPs and would need to be specifically retrieved from their data banks.

- Delays by the industry in seeking access to the information made it more difficult to retrieve and more unreliable; it might be impossible, due to the passage of time, to link some IP addresses to account holders.

- At best the ISPs will generate the name of the account holders, but they can never generate the name of the actual computer users.

Broader privacy concerns were also central to the Court's decision, but Federal Court Justice von Finckenstein acknowledged the limits to the protection offered by privacy legislation. It was "unquestionable but that the protection of privacy is of utmost importance to Canadian society...However while the law protects an individual's right to privacy, privacy cannot be used to protect a person from the application of either civil or criminal liability."

Justice von Finckenstein concluded that the plaintiffs had not made out a *prima facie* case (including a causal link between pseudonyms and IP addresses). Nor had they established that the ISPs are the only practical source for the identity of the pseudonyms or that the public interest for disclosure outweighs the privacy concerns in light of the age of the data.

The court concluded that under the circumstances, given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, privacy concerns outweighed the public interest concerns in favour of disclosure.

The decision was consistent with an admittedly unscientific online poll conducted in February by Toronto's *Globe and Mail* newspaper. Only 12 per cent of respondents thought that ISPs should be required to turn over to the music industry the names of ISP customers who swap songs.

Representatives of the Canadian music industry have now filed an appeal against the judgment.

The Canadian Federal Court's response, however, was not unique. In December 2003, a United States appeal court ruled that the recording industry could not rely on the subpoena provisions of the Digital Millennium Copyright Act to compel ISPs to disclose the names of subscribers whom it had reason to believe were infringing its members' copyrights.

i

FURTHER INFORMATION: For a copy of the ruling, see: www.fct-cf.gc.ca/bulletins/whatsnew/T-292-04.pdf

Sweden opts-in to EU spam rules

Jim Runsten looks at Sweden's new e-marketing regulations, their implications for B2B advertising, how they will apply to marketers located outside Sweden, and how the rules will be enforced.

Article 13 of the 2002 EU Directive on Privacy & Electronic Communications (which regulates e-marketing), was implemented in Sweden on March 3rd 2004 when the Parliament passed a bill on amendments to the Swedish Marketing Practices Act (1995:450) concerning unsolicited marketing via e-mail. The amendments entered into force on April 1st 2004.

INDIVIDUAL SUBSCRIBERS

The new regulations introduce an opt-in regime for individual subscribers. Direct marketing material may not be sent by e-mail to individual subscribers unless recipients have previously notified their consent.

There is an exception to the opt-in regime, which allows the continued use of an opt-out (which can be referred to as a "soft opt-in") provided that the direct marketing is:

- only applied to marketing contacts with whom there has already been a sale
- carried out by the same legal entity that obtained the individual's details
- limited to similar products and services
- to an individual who has not objected to the use of their e-mail address for direct marketing, and who was offered an opt-out when their details were first obtained and for each occasion the details are used for direct marketing.

(Consequently, all the fore mentioned criteria must be met for the soft opt-in alternative to be applicable.)

Registers and lists that have been purchased from third parties do not qualify to fall under the soft opt-in exemption.

Direct marketers should note that the opt-in rule is not limited to "consumers". It applies to all non-corporates - ie. partnerships and sole traders have the same rights as private individuals. Accordingly, the new regulations do to some extent apply to B2B marketing.

The opt-in rule applies to "unsolicited" direct marketing via systems without personal contact. The Swedish Legislator has chosen to keep the opt-out rule for other methods of remote communication (eg. telemarketing) in the new regulations.

> If the soft opt-in exemption cannot be relied on, then strictly speaking the marketer would need to re-approach legacy contacts to obtain opt-in consent with the risk of getting very few positive returns.

CORPORATE SUBSCRIBERS

The opt-in rule does not apply to corporate subscribers. These include companies and other organisations that are legal entities.

However, the new regulations prescribe that all direct marketing must contain a valid address to which recipients, whether a physical or legal entity, can send a request to the marketer to stop sending them marketing material. Where the sending of marketing material to an employee of a company includes the processing of personal data (as it would where the direct marketer knows the name of the person they are contacting - eg. fred@acorporate.com, not dataprotection@acorporate.com), then that individual also has a right under the Swedish Personal Data Act to request that the marketer cease sending him marketing material.

E-MAIL OPT–OUT REGISTERS

Article 7 of the Electronic Commerce Directive (2000/31/EC) allowed for a possible "opt-out" register for unsolicited commercial e-mails. Although, in the regulations that transposed the Electronic Commerce Directive into law, the Swedish Legislator included a rule stating that marketers must check e-mail addresses against existing "opt-out" registers, no such register was ever created. Since all individuals have to opt-in according to the new regulations and it is considered that industry opt-out schemes are sufficient, the new regulations do not prescribe an opt-out register. In any event, most spam originates outside the European Economic Area (EEA) and EEA e-mail registers are peripheral to that traffic (and possibly even counter-productive since unscrupulous spammers may harvest the registers for active e-mail addresses).

NO CONCEALED IDENTITIES

According to the new regulations, marketers must not conceal their identity when they send or instigate the sending of marketing e-mails – whether to corporates or individuals. Marketers must also always provide a valid address to which the recipient can send an opt-out message.

HISTORIC DATA

The new regulations apply equally to new data collected after April 1st 2004 and to historical or "legacy" e-mail data that was collected before that date. Such legacy data for direct marketing to individual subscribers may continue to be used only if it falls within the provisions of the soft-opt-in exemption. If the soft opt-in exemption cannot be relied on, then strictly speaking the marketer would need to re-approach the legacy contacts to obtain opt-in consent with the risk of getting very few positive returns.

Territorial application

The Swedish Consumer Agency is the supervisory authority for the Swedish Marketing Practices Act of which the new regulations will form a part. The Consumer Agency and its Director General, the Consumer Ombudsman, will apply the new regulations to all marketing activities directed to the Swedish market in accordance with a position statement regarding e-commerce and marketing on the Internet made in October 2002 (see notes).

Although the Swedish Consumer Agency is responsible for enforcing the new regulations, it should also be noted that any data processed in Sweden or transferred from Sweden, that falls under the Swedish Personal Data Act is monitored by the Swedish Data Inspection Board.

Enforcement

Both individuals and legal entities may seek remedy from the marketer for breach of the regulations. There are three types of remedies:

- an injunction against continuing the marketing activities under penalty of a conditional fine
- compensation for damages; and
- a fine for disruptive marketing practices.

The Consumer Ombudsman may take enforcement action on his own initiative, or as a result of a complaint by an affected person. The Consumer Ombudsman may demand an order for the marketer to provide information or an injunction against continuing marketing activities under penalty of a conditional fine in the Swedish Market Court. The Consumer Ombudsman can also demand, in the District Court of Stockholm, that the marketer is ordered to pay a fine for disruptive marketing practices if the marketer, or any person acting on its behalf, intentionally or negligently breaches the rules - for example by not providing a valid address in marketing e-mails.

Orders and injunctions combined with a conditional fine may be issued by the Consumer Ombudsman himself in less serious cases. However, what constitutes cases of minor importance is not defined in the Marketing Practices Act. All orders and injunctions issued by the Consumer Ombudsman can be appealed to the District Court of Stockholm, except orders to submit information.

i

Author: Jim Runsten is a senior associate in law firm Bird & Bird's Stockholm office. He can be contacted at: jim.runsten@twobirds.com.

Further information: The Consumer Ombudsman's position statement on e-marketing can be found at: www.konsumentverket.se/Documents/in_english/nordic_statement_ecommerce_2002.pdf.

EU report addresses harmonised e-marketing

In March this year, the EU Article 29 Data Protection Working Party (a group representing EU data protection authorities) published a report on the implementation of the Privacy and Electronic Communications Directive. The directive, which was due to be implemented by all 15 EU member states by November last year, restricts marketers' ability to contact potential customers by requiring them to gain prior (opt-in) consent before sending them advertising via new media channels such as e-mail, SMS and fax.

Despite the intention of creating a harmonised approach to e-marketing within the EU, discrepancies in the way some countries have implemented the directive into national law (as well as failure by others to actually implement the directive on time) has created an uneven approach to compliance. As a result, the Article 29 Working Party has issued its position regarding the steps needed to establish a "uniform application" of the directive.

One of the issues discussed is the methods organisations can use to obtain 'prior consent' from consumers. The Working Party has called for industry associations to develop and promote specific measures for collecting consent.

The Working Party has also stated that marketing via third party lists that were compiled prior to the new opt-in requirement "may in principle not be used". This, however, conflicts with guidance from the UK Information Commissioner which states that legacy data bought from list brokers can be used, provided that the UK Data Protection Act has been complied with.

Another complex issue raised by the Working Party is the distinction made between marketing to individual and business ('legal person') subscribers. Under the E-Privacy Directive, member states were given the scope to develop their own approach to the issue. However, the Working Party notes that this has been problematic, pointing out that while some countries (for example, Germany and Italy) have extended the 'opt-in' rule to business subscribers, others such as the UK and Ireland have adopted a two-tier approach. The Working Party recommends that in countries where marketing to business contacts is permitted on an opt-out basis, "practical rules" should be developed to ensure that organisations are aware of the nature of the people they are marketing to, and that individuals' opt-in rights are respected.

For a full copy of the report, see: http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2004/wpdocs04_en.htm

Report by Alan Pedersen

EU plans to harmonise notification rules

Notifying your data processing activities with national regulators is a burdensome task, one that is made demonstrably harder considering the inconsistent approach taken by EU member states. **Laura Linkomies** looks at the efforts being made to simplify the process.

Differences in member states' notification systems are placing a significant burden on data protection managers' workload. Time spent on filling in forms and checking out what is required in each country could be spent more effectively on other aspects of compliance.

Additionally, data protection authorities in many countries are forced to dedicate much of their workforce just for the purpose of administering their notification systems. It is a problem that has recently been acknowledged by the European Commission, and a subgroup of the EU Article 29 Data Protection Working Party has launched an initiative to examine how notification rules could be simplified and harmonised.

A European Commission official explained to *PL&B International*: "Most Data Protection Commissioners are very supportive of this initiative, and we expect a substantial outcome. In order to achieve this, there is no need to amend the [EU] directive itself, but explore the flexibility of the current systems, and possibly amend national laws. Whereas there are some traditional systems as in France and Spain, as opposed to the more flexible ones such as Sweden, for example, there is no preferred country."

Difficulties in creating a harmonised approach to notification can be expected, especially as some national authorities do not even agree on the basic definitions of data protection terminology. However, as the issue has been listed in the European Commission's action programme for 2004, it is hoped that the work will be completed this year. But, if the Working Group does not produce the results, the Commission has indicated it is prepared to take over and carry on the work.

IDENTIFYING THE PROBLEMS

The European Commission has voiced a number of serious concerns about the implementation of the EU Data Protection Directive. Its 2003 report on the status of implementation across the EU included recommendations for simplifying the notification process. The Commission recommends a wider use of the exemptions for notification - for example, organisation that appoint a data protection officer are not required to notify. The Commission's report also calls for the Data Protection Working Party to examine opportunities to facilitate notification, especially for multinational businesses that operate in several different EU countries.

The report, which is based on feedback from business and data protection authorities, states that:

> "many submissions argue for the need to simplify and approximate the requirements in member states as regards the notification of processing operations by data controllers. The Commission shares this view, but recalls that the [EU] directive already offers the member states the possibility to provide for wide exemptions from notification in cases where low risk is involved or when the controller has appointed a data protection official. These exemptions allow for sufficient flexibility while not affecting the level of protection guaranteed. Regrettably, some member states have not availed themselves of these possibilities. However, the

What is data protection notification?

Under the EU Data Protection Directive (see Articles 18-21), organisations are required to register their data processing activities with the privacy regulators in each EU country in which they operate. The categories of information that organisations are required to notify include:

- Name and address of organisation (or its representative).
- Why the data it holds is being used or processed.
- Who the information relates to (eg. customers, employees).
- Who the data is disclosed to.
- Whether the data is transferred outside the EU/EEA.
- A general description of security measures.

Notification registers are generally updated on an annual basis with entries made freely available to the public.

The directive does provide a number of exemptions to the notification process. For example, an organisation which appoints a data protection officer or only processes 'low risk' data is exempt from the notification process.

In cases where data protection authorities consider the use of personal data to be a 'high risk' (for example, where an organisation processes sensitive information such as genetic or other health-related data), they can require organisations to obtain prior authorisation before carrying out the processing activity.

> Commission agrees that, in addition to wider use of the existent exemptions, some further simplification would be useful and should be possible without amending the existing Articles."

Currently, differences between the EU countries' notification systems are significant, especially with regard to prior checking - eg. in cases of high risk data the data protection authority can require prior authorisation - the use of in-house data protection officials, and the categories of information that organisations are required to include in their notification entries.

WHAT ORGANISATIONS ARE FACED WITH

A study on the implementation of the EU directive by Professor Douwe Korff of London Metropolitan University provides a useful summary on the main differences in EU notification systems. For example, in the case of prior checking, the situation varies from one extreme to another. Whereas in the UK no processing is subject to prior authorisation, in France all public sector processing must be subjected to the data protection authority's approval. Most other countries require prior checking for the processing of sensitive data. However again, the specific details on this are different.

The directive provides for wide exemptions in cases where low risk data is involved, or where the organisation has appointed a internal data protection officer. This is the case in Sweden and Luxembourg, while Germany's data protection law also provides a similar exemption, although it is more limited in its scope. The use of this exemption is to be discussed further at the EU level, as it is recognised that it would allow data protection authorities to devote more of their resources to other tasks.

> "In each country, we have a data protection representative who takes care of notification as part of their jobs in IT, human resources or finance."
>
> **- David Trower, chief privacy officer, IMS Health**

There are also major differences in how manual filing systems are treated. While Denmark, Greece, Italy and Luxembourg require notification of both automated and manual processing operations, some countries extend notification only to some manual systems, while others provide wide exemptions.

There are also differences in publicising the processing operations. Whereas all countries require the details mentioned in the Data Protection Directive (Art 19), some also expect to be informed of additional notifiable particulars. For example, in Austria, data controllers have to define the legal basis for any processing. Denmark requests dates for when the processing starts and finishes, and in Finland, data controllers must inform the authority of the logic behind any fully automated "significant" decisions. The French and German laws, on the other hand, require notification of the retention periods of the data.

TOO MUCH EFFORT, VERY LITTLE BENEFIT

Experts question what value notification schemes have in promoting privacy compliance. It is a well-known fact that notification is widely ignored by organisations and according to Korff, many data protection authorities would prefer to spend their resources on more effective compliance measures. There is the view that notification may even have a negative effect on compliance, as companies could easily come to the conclusion that once they have notified, they are complying with the law. However, some data protection authorities regard notification as having an educational role, as it forces companies to examine their data processing operations against their legal obligations.

> many data protection authorities would prefer to spend their resources on other measures which could contribute more effectively to compliance.

MANAGING NOTIFICATION ACROSS THE EU

IMS Health, an information and analysis provider for the healthcare sector, is a good example of a multinational that processes personal data across many European jurisdictions. "Notification is just one of the issues that is difficult to manage," says David Trower, chief privacy officer at IMS Health. "IMS has operations in all EU countries apart from Denmark and Luxembourg, and we have chosen to deal with notification locally in each country. It would just be too difficult to handle all notifications centrally."

"In each country, we have a data protection representative who takes care of notification as part of their jobs in IT, human resources or finance. There is a company procedure to follow, and if representatives have any queries, they can contact myself, or a local lawyer. The common procedures include ready-prepared forms for assessing compliance needs against the notification rules."

Trower welcomes the intention to harmonise notification rules, but is doubtful about how much common ground can actually be found. He adds that the system IMS has adopted has worked well, but he would prefer notification systems with less bureaucracy. "The notification rules in France, in particular, always seem to cause some concern, as there are very few exemptions in the French rules."

i

AUTHOR: Laura Linkomies is a contributing editor to *PL&B* newsletters.

FURTHER INFORMATION: For a copy of Professor Douwe Korff's *Study on Implementation of Data Protection Directive*: http://europa.eu.int/comm/internal_market/privacy/studies_en.htm

EU survey outlines privacy state of play

Less than a decade after the introduction of the EU Data Protection Directive, the European Commission has conducted a major survey into consumer and business perceptions of privacy legislation throughout the EU. **Lilly Taranto** examines the findings and looks at the implications for businesses operating in Europe.

The European Commission's survey, published in March this year, is divided into two sections: the first part concerns organisations' perception of data protection law, while the second presents the findings relating to individuals' awareness of, and attitudes towards, privacy issues.

BUSINESS PRIVACY PERCEPTION

The first section of the Commission's survey solicited responses from over 3,000 people who were responsible for privacy compliance, including data protection officers and IT, HR and marketing managers. Differences in business attitudes to data protection varied from country to country, depending upon how member states had implemented the Data Protection Directive. There were also differences between industry sectors.

The survey covered the following topics:

- the perception of existing data protection legislation
- internal data protection compliance; and
- how companies perceive non-compliance with existing legislation.

PERCEPTION OF EXISTING LAW

A majority of respondents (54 per cent) rated the level of protection offered by their respective data protection laws as 'medium'. Although this finding was generally the same across all EU countries, there were differences with regard to the industry sector and size of the company involved. The service sector rated the level of data protection as 'high', whereas the construction sector rated the level 'low'. Moreover, larger organisations tended to regard the level of data protection as high.

The results imply that data protection has penetrated business culture and is deemed important in most businesses, especially larger organisations. However, the results suggest that there is a need for more data protection information and training to help bring their business practices in line with national and European legislation.

The high level of data protection awareness is reaffirmed by the fact that the vast majority of companies (91 per cent) agreed that data protection legislation is necessary to safeguard consumers' rights.

Nearly half (44 per cent) of the respondents believed that harmonisation of EU data protection laws is not sufficient. This view was prevalent across all EU countries, especially in larger companies and where the respondents came from marketing departments. It demonstrates that many organisations see data protection as limiting the free movement of personal data and obstructing their business processes. It reinforces the need for national authorities to work together to ensure harmonisation and reduce the differences in their legal approaches.

INTERNAL PRIVACY COMPLIANCE

Respondents to the survey were asked whether they used 'Privacy Enhancing Technologies' (PETs). Less than a third of respondents (32 per cent) indicated that they used this kind of technology - the sector with the highest use of PETs was the service sector. This finding implies that companies are resistant to PETs probably because of the perceived limitations that these technologies may impose, but also because of the costs involved. However, these technologies would highly benefit companies by enhancing legal compliance.

Only one in ten respondents indicated that their company transferred data outside the EU. The highest levels of transfers occurred in larger companies and in the industrial sector. Customer data was the most common type of information transferred overseas (52 per cent). The low level of transfers outside the EU suggests that most transfers occur either nationally or within the EU.

Most respondents indicated that much of the information they are required to provide to customers is not made available to them. Less than half informed consumers about their right to access personal data or provided details on how their information will be used. Larger companies tended to be more upfront as they are exposed to a greater number of customers and are processing large quantities of data. Only 37 per cent of respondents said their organisations reveal the contact details of the person within the organisation responsible for data protection compliance and only 31 per cent replied to individuals' requests.

These findings show that compliance with data protection legislation is far from being achieved, since only larger companies tend to be compliant. This is exacerbated by the low level of complaints. Only 4 per cent of respondents indicated that they had received a privacy-related complaint. This translates into a low incentive for companies to become compliant.

PERCEPTION OF NON-COMPLIANCE

39 per cent of respondents believed that it is the lack of knowledge of data protection legislation that accounts for non-compliance. 28 per cent indicated that deliberate non-compliance is due to the lack of enforcement action taken by national regulatory authorities. Some (17 per cent), however, believed it is due to the fact that companies' adaptation to the new requirements is time consuming – a view that was more

prevalent among larger organisations. Finally, only nine per cent indicated that it is due to the lack of flexibility in data protection law. These findings imply that there is a strong need for education and training to improve knowledge and highlight good compliance procedures.

INDIVIDUALS AND DATA PRIVACY

The second part of the European Commission's survey looked at citizens' views on how companies protect their personal data, questioning over 16,000 people across the EU.

Interestingly, the survey revealed that fundamental variations in attitudes towards privacy issues were based on a country-by-country basis, rather than on a particular socio-demographic characteristic. This implies that data protection is deemed more important in some EU countries than in others.

The results of the survey covered individuals' level of trust in organisations (such as banks and insurance companies, mail order and market research companies), their attitudes towards privacy, and their knowledge of data protection legislation.

LEVELS OF TRUST

On average, 60 per cent of individuals were concerned about the protection of privacy with deep variations between countries – only 9 per cent were concerned in Greece, whereas 38 per cent were concerned in Finland.

Individuals' trust varies from sector to sector. 48 per cent of individuals do not trust insurance companies and banks, although this figure differs between countries. 71 per cent of Greeks, for example, do not trust insurance companies and banks, but 77 per cent of Finns do. The variation in results could be because some countries have had high profile cases involving the financial services sector which has raised the public's awareness of privacy.

The results show that the banking and insurance sector needs to invest internally and externally to become more trustworthy and legally compliant. Good compliance practices will help to avoid business risks such as fines, negative PR, and damaged reputation to the financial services sector in general.

The importance of investing in legal compliance is also relevant for employers, market research companies and, to a greater extent, for mail order companies. The belief that employers could be trusted to use personal information in an acceptable way was held by 55 per cent of individuals polled. Danish organisations were the most trusted employers. Although mail order companies' image has improved slightly over time, their use of personal information is still not trusted by 68 per cent of individuals across the EU, and this figure rises to 75 per cent in France.

Market research companies were trusted by 43 per cent of individuals polled, with high levels of trust in Denmark, but low levels in Ireland.

Companies maintain that compliance is time consuming and the low rate of prosecutions discourages them from becoming compliant.

VIEWS ON PRIVACY

Nine out of ten individuals agreed that they should be informed why organisations are gathering their data and whether they share it with third parties. This result was high in all EU countries and demonstrates that there are high levels of concern. The results imply that organisations handling personal data must be more effective in providing individuals with information on how they process and control their data.

KNOWLEDGE OF PRIVACY LAW

The survey found that while most individuals said that the level of protection provided by data protection laws was high, they also indicated that general levels of awareness were rather low. This implies a need to provide more education and information to individuals on data protection legislation.

This need is confirmed by another set of results regarding individuals' knowledge of their rights, which reveal that individuals have low awareness of:

- the existence of national data protection authorities (68 per cent unaware)
- the right to access and correct data (68 per cent unaware - only 7 per cent of those that were had exercised this right)
- the right to know why their details are being collected (58 per cent unaware)
- the right to opt-out from marketing contact (51 per cent unaware); and
- the right to consent to certain types of processing (51 per cent unaware).

CONCLUSIONS

The findings of the survey indicate that businesses are willing to become compliant and that individuals are concerned about their personal data. However, both individuals and businesses do not have a sufficient level of awareness of data protection legislation. Companies maintain that compliance is time consuming and the low rate of prosecutions discourages them from becoming compliant.

Despite the lack of incentives, companies must become compliant to avoid business risks linked to negative PR, obtain individuals' trust and, as a result, acquire more customers. An incentive for companies to become compliant could derive from individuals' improved knowledge of the law and their rights. Individuals who are better educated and informed about privacy would be more likely to exercise their rights and demand that organisations adopt robust compliance practices.

However, national authorities will have to invest more resources in data protection education and information in order to ensure higher levels of compliance across the EU.

i

AUTHOR: Lilly Taranto is a consultant at Marketing Improvement. She can be contacted by e-mail at: lilly.taranto@marketingimprovement.com.

FURTHER INFORMATION: The European Commission's data protection survey can be found at: http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm#actions

South Africa edges towards data protection legislation

The South African government is expected to publish a draft data protection bill by the end of this year, although when legislation will finally be passed is still unclear. **James Michael** outlines the developments and suggests that demands from the European outsourcing sector could provide the incentive to move forward.

Although South Africa's data protection legislation was supposed to be simultaneous with freedom of information, the Promotion of Access to Information Act became law in 2001, while data protection will only reach the stage of a draft bill at the end of 2004.

Data protection originally had been more closely connected with freedom of information legislation than in most countries (but not all, eg. France and Canada's nearly simultaneous national access to information and privacy laws). It started with the Interim Constitution in 1993 which became, with modifications, the Constitution in 1996. Both the Interim and the final Constitutions had provisions establishing the right to personal privacy. They also both had provisions establishing the public right of access to information.

During the Mandela presidency (1994-1999) there was an inquiry into the related questions of access to government information and privacy. Instead of being referred to the South African Law Commission (now the South African Law Reform Commission) the matter was referred to a committee chaired by the then-Deputy President, and now President, Thabo Mbeki.

They reported in 1996 with the Open Democracy Bill, which was introduced into Parliament in 1998, withdrawn, and re-introduced in 1999. The bill included four parts: one establishing a public right of access to information, the second establishing open meeting rules, the third providing protection for disclosures in the public interest, and the fourth providing privacy protection for personal information under government control.

The constitutional right of access to information had been interpreted by the Constitutional Court as requiring the constitutional provision to take direct effect if implementing legislation was not law by February 3rd 2000. In December 1999 it became obvious that the Open Democracy Bill could not complete all the parliamentary stages by February, and the whistleblower protection, open meetings, and privacy protection sections were removed so the access to information section could become law by the deadline. The whistleblower protection section later became law as the Protected Disclosures Act 2000. The original privacy protection section was not really a data protection law in the sense of the Council of Europe Convention or the EU Data Protection Directive, being closer to the original US and Canadian Privacy Acts. So, the government started over again on data protection.

> The timing of the data protection bill could well be influenced, as it has been in India, by the growth of information technology outsourcing in South Africa from Europe.

Privacy consultation

The subject of privacy and data protection was referred to the South African Law Commission in 2002, which appointed a committee to consider the matter (Project 124). In August 2003, the committee published its Issue Paper and asked for comments by the beginning of December 2003. They are now examining the comments received and will publish a further Discussion Paper, including a draft bill, around the end of 2004. The Issue Paper reviews the history and theory of privacy law, considering common law protection in South Africa through the general civil remedy for invasion of privacy and other related wrongs, and the Constitutional protection.

Data protection is described in terms of international measures and national legislation, including the Council of Europe Convention, the OECD Guidelines on privacy, the EU Directive, the UN Guidelines, and the Commonwealth Model Bills. National legislation is noted, including subject access under the Promotion of Access to Information Act, and encouragement of voluntary data protection under the Electronic Communications and Transactions Act.

Approaches to data protection regulation

The paper identifies four models of data protection: comprehensive laws, sectoral laws, self-regulation, and technology. The Commission emphasises that: "It is clear that the process of establishing policy goes beyond the level of basic statutory data protection principles to include the ways in which these principles should be enforced, eg.

through supervisory authorities."

As a starting point the Commission proposes that the next stage of the investigation should include automatic and manual files, information about both natural and legal persons, information kept by both the public and private sector, and both sound and image data. The inclusion of information about both natural and legal persons (ie. companies) is because of the limited recognition in South African case law of a corporate privacy right. Extension of data protection legislation in South Africa to legal persons would be unusual, but not unprecedented.

OUTSOURCING IS AN INCENTIVE

The question of when that bill will be introduced and when it is likely to become law is a matter of political priorities. The timing of the data protection bill could well be influenced, as it has been in India, by the growth of information technology outsourcing in South Africa from Europe. Call centres, for example, have been growing rapidly in the past few years in South Africa, aided by an Anglophone and IT-literate population, the same time zone as Europe, and a low wage economy.

If the EU Data Protection Working Party turns its attention to examining whether data protection in South Africa is 'adequate' in terms of the EU Directive, it could be a significant incentive to rapid legislation. Thus far, the Working Party has made adequacy findings on Switzerland, Hungary, Canada, the US Department of Commerce Safe Harbor Principles, and Argentina, with Australia and New Zealand heading its programme of work for 2004.

AUTHOR: James Michael is a Senior Research Fellow for the Institute of Advanced Legal Studies, London University, and a professor at the University of Cape Town.

India commits to data protection, continued from p.3

EU than it does with the US and that its population is around three times larger than that of the US. But it is doubtful that the European Commission will devote the time and resources needed to pursue this option. One reason is that a safe harbor agreement with India could spark off requests for similar arrangements with several other countries. In any event, critics of the safe harbor arrangement argue that it is a poor substitute for a law.

4. Amend the IT Act - Acharya explained that India's IT Act 2000 addresses utilisation of IT, covering issues such as hacking and other forms of cybercrime. Section 43 of the law makes provision for claiming up to 10 million Rupees ($225,000, €190,000) in compensation for breach of the law. It would be possible to add an amendment to cover data protection.

Pavan Duggal, who drafted the IT Act, explained to *PL&B International* that the IT Act has three main objectives:

- legalise business conducted electronically
- facilitate e-filing of documents with government agencies; and
- provide consequential amendments to certain other laws, such as the Penal Code and the Evidence Act.

For the first time in India, this law provides a definition of "data" and "information" and so provides a convenient existing vehicle for a new data protection section.

5. A Data Protection Ordinance - Duggal explained that a further option for the government is to adopt a Data Protection Ordinance. The advantage is that it could be introduced with immediate effect. The disadvantage is that it would need to be ratified by both houses of the legislature within six months, otherwise it would cease to have effect. Such an outcome would be embarrassing for the government. A further disadvantage is that data protection is not a subject which requires such immediate action. It would be better to achieve consensus and support from the interested parties. This approach would be more likely to work effectively in practice.

6. A specific data protection law for the private sector - There is little support for this option because there is no perceived need in India from the business perspective. Another problem with this option is that it would take valuable and scarce parliamentary time to introduce such a law and could take up to two years to pass through all its legislative stages.

Whichever option emerges from this process, it is unlikely to follow any existing national model. Instead, it would need to address the specific Indian context. Any data protection initiative would not be aimed at the domestic context but rather the business process outsourcing sector.

Questions which the IT Ministry's advisory committee will need to address include:

1. If the government goes ahead with any of the data protection proposals, it needs to consider whether it would use current or new oversight and enforcement agencies.

2. Would the compensation provisions of the IT Act be extended to breaches of individuals' privacy or data protection 'rights'?

Both Duggal and Acharya expect more clarity on the government's way forward to emerge soon after the forthcoming election. The CII's Acharya summarised the consensus of all domestic parties to India's data protection debate. "Economic growth is vital to the mass of India's population. Nothing should be done to harm that growth."

KEY CONTACTS: Pavan Duggal Associates, New Delhi, India (E-mail: pduggal@nde.vsnl.net.in; Website: www.cyberlaw.net)

Anindya Acharya, Deputy Director for IT, Business Process Outsourcing and E-Commerce at the CII can be contacted at: anindya.acharya@ciionline.org

For details on India's IT Act 2000, visit the Ministry of IT website at: www.mit.gov.in

Common law privacy torts - paper tiger or new limit on corporate behaviour?

Eugene Oscapella examines whether the use of privacy torts to seek legal redress poses a threat to the business community.

A recent Court of Appeal decision from New Zealand has confirmed the emergence of a common law (judge-made) tort of invasion of privacy in that country. The existence of such a tort gives individuals a right to take civil action in the ordinary courts against companies, individuals and sometimes governments, for damages or injunctions.

At first glance, the Hosking decision, released March 25th 2004, may appear to be only of local interest. Decisions of New Zealand courts do not bind courts of other countries. However, even if not binding on other common law countries, the decision may encourage judges abroad to be more inventive in addressing privacy issues, with consequences for corporate behaviour in those countries. At the same time, some question the practical impact of a privacy tort on corporate behaviour. Even if a full-fledged privacy tort emerges, is it largely a legal right in theory only — a paper tiger?

The Hosking decision involved a photographer who, without the consent of two "celebrity" parents, took pictures of the couple's children in a public street. The couple sought to prevent publication of the photographs in a magazine.

The majority of the Court of Appeal concluded that it was actionable as a tort to publish information or material in respect of which the plaintiff has a reasonable expectation of privacy, unless that information or material constitutes a matter of legitimate public concern justifying publication in the public interest. However, the majority also found that neither the parents nor the children had a reasonable expectation of privacy in the circumstances of the case.

DP LAW, CONSTITUTIONAL RIGHTS AND PRIVACY TORTS

The Court found that New Zealand's Privacy Act was no impediment to the creation of a common law privacy tort. Justice Tipping stated that, "In the absence of any express statement that the Privacy Act was designed to cover the whole field, Parliament can hardly have meant to stifle the ordinary function of the common law, which is to respond to issues presented to the Court in what is considered to be the most appropriate way and by developing or modifying the law if and to the extent necessary."

The Court also rejected the notion that the absence from the Bill of Rights Act of a broad right of privacy inferred against incremental development of the law to protect particular aspects of privacy that may evolve case by case. Said Justice Tipping, "Society has developed rapidly in the period of nearly 15 years since the enactment of the [New Zealand] Bill of Rights in 1990. Issues and problems which have arisen, or come into sharper focus, as a result of this development should, as always, be addressed by the traditional common law method in the absence of any precluding legislation."

EXTENSION OF THE TORT

The judgment is quite clear that it was not intended to extend the scope of the tort of invasion of privacy beyond the circumstances of the case — unwanted publication of photographs by a magazine. However, the reasoning behind the creation of the tort could well serve as a springboard for lawsuits by those with other privacy concerns that are not addressed by current laws. As Justice Gault noted, "The law governing liability for causing harm to others necessarily must move to accommodate developments in technology and changes in attitudes, practices and values in society." Furthermore, he noted, "from time to time . . . there arise in the courts particular fact situations calling for determination in circumstances in which the current law does not point clearly to an answer. Then the courts attempt to do justice between the parties in the particular case. In doing so the law may be developed to a degree."

Applying Justice Gault's reasoning, video surveillance of employees and customers, use of RFID (radio frequency identification) tags and employee drug testing are among the many situations where privacy torts could fill a gap in the law. Consumers might also rely on the tort to challenge data collection and handling practices, even if the practices comply with data protection legislation. Thus, companies might not only have to comply with data protection laws, they might also have to ensure other aspects of their operations respect the somewhat amorphous notion of a right to privacy.

PRIVACY TORTS ELSEWHERE

The Hosking decision also contains a very useful comparative survey of the current state of the law on privacy torts in several other common law jurisdictions — Australia, England, the United States and Canada.

Australia - The Court in Hosking noted that there were some early indications that a privacy tort might be introduced in Australia in media cases. However, later courts have declined to recognise a stand-alone common law right to privacy in Australian law. Justice Gault concluded that, "essentially . . . the High Court of Australia has not ruled out the possibility of a common law tort of privacy, nor has it embraced it with open arms. Nor did current Australian legislation such as the Privacy Act 1988 (Cth) create a statutory tort of privacy (a statutory tort of privacy creates a right of civil action for violations of privacy through legislation rather than through common law)."

United Kingdom - The Court remarked that there was no common law tort of privacy in English law at present. However, the tort of breach of confidence provided a right of action to both companies and individuals in respect of use or disclosure where information has been communicated in confidence. As well, the tort of breach of confidence gave a cause of action in respect of the publication of personal information about which the subject has a reasonable expectation of privacy.

Justice Gault observed that the Human Rights Act 1998 incorporated the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 into domestic law. Article 8 of the Convention provides that everyone has the right to respect for his private and family life, his home and his correspondence. The result, he suggested, has been the continued evolution of the existing breach of confidence action in the UK to address privacy concerns.

United States - The Court in Hosking also reviews the US jurisprudence and literature on privacy torts. It refers to the Restatement of Torts, which sets out the broad parameters of the tort of privacy in the US:

1. One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

2. The right to privacy is invaded by:

a. unreasonable intrusion upon the seclusion of another . . .
b. appropriation of the other's name or likeness . . .
c. unreasonable publicity given to the other's private life . . .; or
d. publicity that unreasonably places the other in a false light before the public . . .

Canada - The Court in Hosking noted that Quebec enacted a "quasi-constitutional" statement of rights that guarantees every person "a right to respect for his private life." This right, found in the Quebec Charter of Human Rights and Freedoms, can be exercised in relations between individuals, between individuals and government, or between individuals and corporations. Thus, companies subject to Quebec law must not only respect data protection legislation, but also the broader privacy protections encapsulated in the Quebec Charter.

The Court in Hosking also noted that several Canadian provinces have enacted statutory privacy torts. (By way of example, British Columbia has a broad statutory tort, making it "actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.")

The New Zealand judgment notes the continuing uncertainty about the existence of a common law tort of privacy in Canada, but hints that the development of such a tort may be close, since "privacy concerns are increasingly receiving protection in Canada."

IMPACT ON CORPORATE BEHAVIOUR

As noted above, the evolution of a common law privacy tort has significant potential implications for relationships between a company and its customers and employees, and even with individuals who have no dealings with the company. The tort introduces a new element of privacy protection for individuals that may extend far beyond the protections afforded by data protection law. However, the scope of this protection will remain unclear until successive judgments flesh out the tort. This creates some uncertainty for companies. The uncertainty about the scope of the tort may also make individuals who feel their privacy has been violated reluctant to rely on the tort to sue a company. For example, will future judges in New Zealand extend the scope of the common law right to privacy enunciated in the Hosking case? Or will they limit the right to the limited circumstances of the case – the publication of photographs of individuals taken without consent in a public place?

RFID technology and employee drug testing are among the many situations where privacy torts could fill a gap in the law

Justice Tipping acknowledged the lack of certainty about the scope of the privacy tort in the case before the Court in Hosking. Still, he argued, there was not much force in the criticism that the new tort is so uncertain that it should never be born. "The parameters of any general duty are constantly being worked out and refined by the Courts," he said. An underpinning jurisprudence could be allowed to develop for privacy. "What expectations of privacy are reasonable will be a reflection of contemporary societal values and the content of the law will in this respect be capable of accommodating changes in those values."

The second factor militating against companies being pursued through common law or statutory privacy torts is the burden of litigation for the complainants. Complaints made under data protection legislation are investigated by data protection authorities at no expense to the complainant. However, an individual who relies on a privacy tort to challenge a company's actions must launch a civil action against the company and incur the expense of litigation against an entity that may have much greater resources. (The Hoskings not only lost their case, but paid their own lawyer's fees and were ordered to pay NZ$18,000 in costs). Thus, only the wealthy (as in the Hosking case) or organisations (including unions and public interest groups) may realistically be in a position to rely on these torts to obtain legal redress.

In fact, Justice Keith, one of two justices in Hosking who argued against the creation of a tort of privacy, stressed the lack of utility of such a tort in practice. He noted that in both Canada and the United States, the tort of privacy has only rarely been invoked. He cited one 1983 study that found fewer than 18 cases in the United States – or about two each decade – in which a plaintiff was either awarded damages or found to have stated a cause of action sufficient to withstand a motion for summary judgment or a motion to dismiss.

Perhaps, as Justice Keith suggested, a privacy tort will cause barely a ripple in the world of privacy protection. However, as individuals become increasingly sensitive to privacy intrusions, and with legislatures often slow to respond to those concerns, companies should not entirely discount the impact of this emerging tort on their activities.

i

FURTHER INFORMATION: For the full judgment of the Hosking case: www.law.auckland.ac.nz/learn/medialaw/docs/Hosking.pdf

Building a culture of privacy at Hewlett-Packard

Hewlett-Packard is one of the pioneers of a new wave of global companies to see privacy as more than just a straightforward compliance issue. **Barbara Lawler**, chief privacy officer at HP, talks to *PL&B International* about her ongoing efforts to build a culture of privacy within her organisation.

"I first came into privacy for Hewlett-Packard really before CPO was on the map as a job title, or job function," says Barbara Lawler. Starting in the summer of 1999, and later formally appointed as CPO in March 2002, Lawler took up the privacy mantle at HP at a time when data protection was still a relatively low priority issue for businesses. E-commerce was still in its infancy, with all the potential and pitfalls yet to be realised. This was before spam, Internet fraud and privacy breaches really captured the public's attention.

Lawler was given the challenge of building a relatively unknown concept into the business culture at HP and initially, she says, people were simply unaware of the enormity of the project ahead. "I had someone say to me: 'Isn't that [privacy] the little statement you see at the bottom of the web page? What will you do with the rest of your day?' - That was the thinking," she says.

The growth of technology and the Internet has enabled organisations – and in particular marketers – to realise the full business potential of information. But with it comes the responsibility to manage that information appropriately – to *use* people's personal data, rather than *exploit* it. And this is where Lawler comes in.

Unlike many CPOs, who tend to be drawn from legal and compliance backgrounds, Lawler comes at privacy from a business perspective. With over 20 years at HP, her experience is grounded in systems and data management and a range of marketing activities - a background that has helped her to break down the barriers between compliance and business development.

"HP wanted someone who spoke the language of the marketer and could understand what they were trying to accomplish, but could also represent the policy needs and obligations of the company," she says. "Having that long time experience in the company and understanding how things got done through the informal as well as formal structures, was a tremendous help for a function and a subject area that was not just new, but foreign to many people in the company."

She explains that there were two key goals behind HP's decision to be an early adopter of privacy management. One was based around the company reputation. The other, was to view privacy as a key element in upholding the values of the organisation, its brand promises of trust and integrity with its customers.

Lawler says that privacy at HP is more than just about compliance risk or reputational issues, it is something that has been woven into the ethics of the company. It is not just about paying lip service to consumer concerns and demands - HP has taken privacy further by incorporating the concept into its global citizenship framework, sitting it alongside other public policy issues like corporate social responsibility, human rights and fair employment practices.

DEVELOPING A PRIVACY FRAMEWORK

One aspect of HP's framework that sets it apart from many organisations is that it splits privacy compliance into two streams, making a distinction between customer and employee data. "When I started we had a fairly long standing employee policy, and there was a working group focussing on calibrating that with the new EU directive," she says. So, one of her first mandates was to develop a framework for customer data that would run alongside the HR policy. "From a customer perspective, this was really a new space so I was chartered to accomplish three things: (1) to build out the implementation framework for the fundamental policy we had around customer data; (2) to do that you need to have a tremendous effort around training and awareness inside the company; and (3) establish the company's approach to privacy as one that sets a leadership example among industry, and within the Fortune 100 as a whole."

Lawler explains that HP laid down a policy framework based on concepts taken from EU data protection principles and BBBonline (the privacy seal provider) requirements. The framework laid down the approach on areas such as consumer notice and choice, data accuracy, access, security and oversight.

This policy was then supplemented by a 'privacy rulebook' which has evolved over time to provide more in-depth guidance on specific areas such as e-marketing, call centre operations, market research and customer focus groups.

A GLOBAL APPROACH TO PRIVACY

Because HP is a global business, its strategy has been to build a standard approach to privacy compliance, adopting the same principles across each of the countries in which it operates. However, Lawler says the global policy still needs to be flexible enough to be able to take into account differences across jurisdictions. "What we allowed for in the rulebook is the need to adapt certain aspects, and that varies from country to country, such as how and when a notice is delivered, what choices are offered, and when and how they are offered."

"It's usually our partners at HP legal that assist us with that. In addition, we have regional-based privacy managers focused on both customers and employees – one for each - that are specialists in these areas."

In Europe, one of the more

complex regions in terms of privacy compliance, Lawler explains that HP's regional managers are further supported by individuals on a country level. It is an approach, she says, that the company is now starting to mirror across other regions such as Asia-Pacific and the Americas.

In marketing terms, HP's approach is to offer its global customers standard choices for marketing – they can choose to receive or opt-out from contact via specific channels such as e-mail, post, telephone or mobile. Additionally, they are also offered a single 'global' opt-out that removes them from all marketing contact.

Lawler explains that although HP's overall standards are global, there is again a need for some country-by-country variation. This is not just because of legal requirements, but also for cultural reasons – for example how customers are communicated to, what language, how often, the style and tone of the message and so on.

She concedes that despite having high privacy standards, recent e-marketing legislation has proved a challenge for HP. This, she says, is mainly because laws such as the US CAN-Spam Act and the European E-privacy Directive contain vague definitions that create confusion for marketers, rather than clarification. "Marketing people, at the end of the day, want to be able to do their project and get the results they're measured on. They want a quick list: a 'what are the five things I need to do to make sure I am compliant, but also meet my business goals."

For employee data HP, again, has an overall global policy, but looking at specific issues on a country-by-country basis is "almost unavoidable" argues Lawler. In Europe, for example, multinationals not only have to contend with different labour laws, but also national variations of what is supposed to be a harmonised set of data protection laws.

"It's a real challenge," she says. "It has created a lot of complexity, and takes a tremendous amount of time if you're going to do it well."

Implementing the framework

A key factor in the implementation of HP's compliance programme, says Lawler, is privacy auditing. "We have an internal audit framework that has a fairly detailed, but also layered set of questions, depending upon the kind of audit that is being conducted by the organisation."

She explains that audits of specific business units - such as marketing, for example - will be more rigorous, drilling deeper into core issues such as consumer notice and choice.

On more general country-based audits, where a number of business functions are examined, a more basic audit is carried out, looking at issues such as staff awareness of the HP policy, and whether they have been trained and understand key privacy principles. If the general audit identifies compliance gaps, says Lawler, they will then probe deeper to discover the underlying causes. "Depending on what they find, privacy staff can then go back and engage with those organisations and help them get to a much stronger compliance level."

She explains that auditing is an ongoing process which is tied to the organisation's overall internal audit schedule. "If there's a particular area that needs to be targeted, we partner with internal audit to make sure that privacy is included in the audits where that is likely to be an issue."

Most business units, she says, will be audited every 18-24 months, although higher risk units are hit once a year. And to complement the internal audit process, HP also uses third party auditors to target key areas of the business, examining compliance levels and assessing any gaps that may exist.

> "HP wanted someone who spoke the language of the marketer and could understand what they were trying to accomplish, but could also represent the policy needs and obligations of the company."

Raising awareness

HP is engaged in an ongoing staff training programme to communicate its privacy goals throughout the organisation. "We have some broad general global training for all employees, and then we also find the inescapable need to provide fairly custom-focussed training. What a call centre needs is very different from what an e-marketing group needs."

"Company wide training for privacy was just recently introduced and that will be a requirement every other year for employees," she explains, "with the exception that there are some specific groups that will need to read up on an annual basis - in situations where they have access to sensitive data from a human resources perspective."

As well as raising awareness, Lawler has addressed compliance risks by putting together a series of tools to help build privacy into new projects and procedures. These include templates for privacy impact assessments (PIAs), application development checklists, and implementation tools. She explains that HP is working towards the target of creating a closed loop process whereby every single new project or programme that touches upon personal data is properly assessed against the organisation's privacy policy - a significant undertaking considering the number of small or one-off projects that are created across organisations as large as HP.

To achieve this, HP has appointed full-time privacy managers in each of its core business units, to provide advice and assistance in implementing privacy effectively into their operations and practices.

Outsourcing relationships

Probably the hot privacy topic at the moment is outsourcing and the relationships organisations have with third party processors. "For many companies like HP, these issues aren't new, they just haven't surfaced in the way that they have now," says Lawler. "We have been looking at outsourcing and vendor contracts for quite some time. This was something we started working on in the first year that I came on board."

Moving quickly and ensuring that proper vendor protection was in place was necessary, not just from the perspective of achieving HP's privacy goals, but also to meet its requirements under the EU-US Safe Harbor scheme, which the company signed up to in January 2001.

Lawler explains that HP employs a mix of vendor agreements depending upon the type of outsourcing relationship. Since late 2000, HP has been incorporating personal data protection agreements (PPDAs) into new contracts and contract renewals. “We also use [EU] model clauses for certain outsourcing arrangements,” she says, “where we have multiple data sources moving to multiple locations.”

“We’ve also added some fundamental privacy language to our master service agreement templates.” She explains that outsourcing relationships will involving drawing up a ‘master’ agreement, with several sub-agreements, of which one will include the PPDA. Inserting privacy elements into the master agreement, she says, helps ensure that every vendor agreement contains a basic level of privacy protection, even in low risk relationships where little personal data is involved.

One of the challenges, says Lawler, has been that the procurement process at HP was spread out across the organisation’s business units, rather than centralised. This has made it harder to ensure that all procurement departments were getting the right information to put into their outsourcing contracts, although she says that following the HP-Compaq merger (see below) the process has now become more centralised.

Lawler says that organisations do, however, need to go beyond contracts and engage with vendors by reviewing their data handling practices and assessing levels of protection. At HP, she explains, this process will either be done at the vendor selection stage, or once an agreement has been signed and the implementation process is being put in place.

PUBLIC POLICY

Another key element of Lawler’s work is based around public policy issues, keeping up-to-date on legislative developments and being the public face of HP’s privacy programme. “Right now I probably spend about 25 per cent of my time on these issues,” she says. Her policy work involves collaboration with HP’s government affairs team to look into privacy developments across a number of regions including Europe, Asia Pacific and Latin America. In addition, she and her colleagues work with industry groups such as the International Association of Privacy Professionals (IAPP) and the European Privacy Officer’s Network (EPON). HP also consults with government officials, privacy regulators and other policy makers to “share with them our strategy and our challenges around managing privacy, but also to hear from them what they see as concerns, what they see as most important for a global business like HP.”

ONGOING CHALLENGES

One major development over the next two years says Lawler will be to drive forward HP’s “design for privacy” initiative, a project aimed at developing a privacy architecture which will ensure that privacy requirements are built into all of HP’s products and service offerings.

Overall, Lawler’s challenge will be to continue the development and realisation of HP’s privacy objectives. “The vision is that privacy will be baked into all our business processes,” she says. “But I would say that is a very long-term vision just because of the volatile nature of business in a global company today – processes and business models change on a fairly rapid basis.”

Tackling privacy in the Hewlett-Packard - Compaq merger

HP’s multi-billion dollar merger with Compaq in 2002 presented a major challenge in terms of merging staff and customer records under one legal entity. One of the objectives was to ensure a seamless merger of the two separate employee databases into one staff directory. The legal problems surrounding employee data and EU data transfer requirements, says Lawler, were eased considerably by the fact that both HP and Compaq were signed up to the EU-US Safe Harbor programme prior to the merger. “That was something that the regulators - both from the European Commission’s side and from the FTC - indicated was one of the positive reasons for supporting and approving the merger,” she says.

Good labour relations also played its part in smoothing over the transition process. “Because HP in particular had such strong relationships with its workers’ councils, we were able to leverage that into getting specific approval from them in advance of day one of the merger, to ensure that we could, with their support and approval, merge those databases and have those available to employees.”

On the customer side, Lawler says they decided to take a best practice approach that would maintain good customer relations. “We took on - and this was beyond what we felt was explicitly mandated in any particular data protection law, although you could argue that there were some countries in the EU that would have expected it - a data transfer notification process for approximately 5.7 million pre-merger Compaq customers.”

HP decided to take a segmented approach to the customer notification process, depending on whether they were high level enterprise customers, SMEs or individual consumers. The large enterprises, for example, were contacted by their accounts teams at Compaq, while lower level customers were notified via a mix of written or electronic communications. Customers were given the opportunity to opt-out from having their details transferred to the new company in addition to a subsequent notification to revalidate their marketing preferences.

Despite concerns in some quarters that there might be high opt-out levels, Lawler says the project was a huge success. Not only did the project come in under budget and within the deadline, but the opt-out rate only reached around 0.5 per cent. “We thought it was truly worth it,” she says. “It showed a lot of respect for those customers and allowed individuals who had strong feelings - either about the merger or about their data being transferred - to have that choice.”

A primer for customer privacy management

Walter Janowski takes a US perspective on how organisations should implement a compliance programme for managing customers' privacy preferences.

Economic pressures are driving enterprises to search for ways to squeeze maximum returns out of their customer relationships, and along the way some enterprises are testing just how much intrusion customers will tolerate. Whether or not these efforts violate enterprises' own privacy policies, they can result in a backlash from customers, privacy advocates and the media.

As enterprises become more aggressive in their marketing efforts and seek ways to circumvent privacy restrictions, the potential for a high-profile privacy-abuse scandal increases. In a climate where the general public is greatly concerned with corporate ethics and accountability, an enterprise that makes a significant misstep in managing its customers' private information could become the "Enron of privacy".

In addition to the potential damage to the enterprise's reputation and brand, it is likely that such an event would drive US government regulation to enact more restrictive privacy legislation along the lines of what has been implemented in the European Union. By 2005, at least one major US enterprise will experience high-profile customer backlash due to the mismanagement of customer privacy information, and public outcry will motivate the US Congress to mandate restrictive privacy legislation.

Given the current state of the economy, privacy management must be prioritised with other investments. Without a serious public breach to serve as a warning, privacy management likely will continue to receive low priority. Thus, when the abuse of customers' personal information by an enterprise leads to a highly visible, public scandal, enterprises will be ill-equipped to respond. Although enterprises cannot forecast the shape that government privacy legislation could take, those that address privacy management concerns today will not only be ahead of their competition, but will also be better prepared to accommodate privacy legislation requirements when they appear.

Without a serious, public breach to serve as a warning, privacy management likely will continue to receive low priority. Thus, when the abuse of customers' personal information by an enterprise leads to a highly visible, public scandal, enterprises will be ill-equipped to respond.

THREE CRITICAL COMPONENTS OF PRIVACY MANAGEMENT

For any enterprise, crafting a comprehensive privacy policy for managing customer data is an important first step in implementing customer privacy management. However, how that policy is implemented and used throughout the enterprise is every bit as important as the policy itself. Here, we define the three critical components of customer privacy management as being able to communicate, enable and enforce a privacy policy.

Communicate — Privacy preferences at the individual customer level must be determined, recorded and distributed where appropriate. Customers may select "opt-in/opt-out" preferences that are applicable enterprise-wide or specific to particular types of communications or channels. Customers also must be able to view and understand an enterprise's privacy policies. They must be able to regularly access their profiles, view their preferences as recorded by the enterprise, and change/maintain these profiles as required. Once collected, the complete set of preferences for each customer must be communicated enterprise-wide, wherever a customer communication might occur. Although the consolidation of customer information into a single data repository is preferable, for many enterprises, customer data is so fragmented enterprise-wide that it would be prohibitive to delay privacy initiatives while waiting for consolidation. In such cases, interactions between databases must be structured so that privacy preferences can be managed from a single access point, but are available wherever customer data is accessed.

Enable — Once customer privacy preferences are established, mid-level marketers should not make decisions as to which customer profiles they can access as marketing prospects. The internal distribution of customer information must be managed by a central, higher-level role (for example, senior marketing manager or chief privacy officer), and must be based on the individual privacy preferences specified by the customers. For example, if a marketer prepares an e-mail marketing campaign, he should not be able to query the entire customer database to determine e-mail preferences to prepare his customer target list. Instead, he should only have permission, from a more-senior level, to access names of customers who have granted e-mail access.

Enforce — Once implemented, an enterprise's privacy policy is useless if its employees don't follow it. Enterprises must implement processes and monitoring technologies to ensure that policies are properly enforced. This can be partly accomplished by restricting data access. However, enterprises also must be able to detect rogue internal initiatives (for example, a department that creates a customer database through independent customer contact) as well as to monitor potential abuses that are technically "within the law" of a privacy policy (for example, a customer who has given permission to be contacted by e-mail becomes the target of an aggressive daily e-mail bombardment).

PRIVACY CHECKLIST

Within the realms of these three critical components, we define a checklist of eight key considerations in privacy policy implementation (see chart below).

Many enterprises consider a privacy policy as an end rather than a beginning. However, once a comprehensive privacy policy is crafted, the challenge of implementation becomes apparent.

COMMUNICATE

Do you communicate your privacy policy to your customers? Obviously, your privacy policy is of no use to your customers if they cannot see it. How is it presented to them? Is it easily accessible? Mailing a tiny, multipage pamphlet filled with fine print and legal terminology may fulfil the technical requirement for customer notification, but it does little to instill customer trust or confidence. Customers should have the opportunity to access your privacy policy anywhere and anytime they want it. Make it accessible from your website and provide copies wherever and whenever there is a customer interaction. The overriding goal is to make it available when it is needed, and it should not be the customer's responsibility to capture and retain it when you choose to send it.

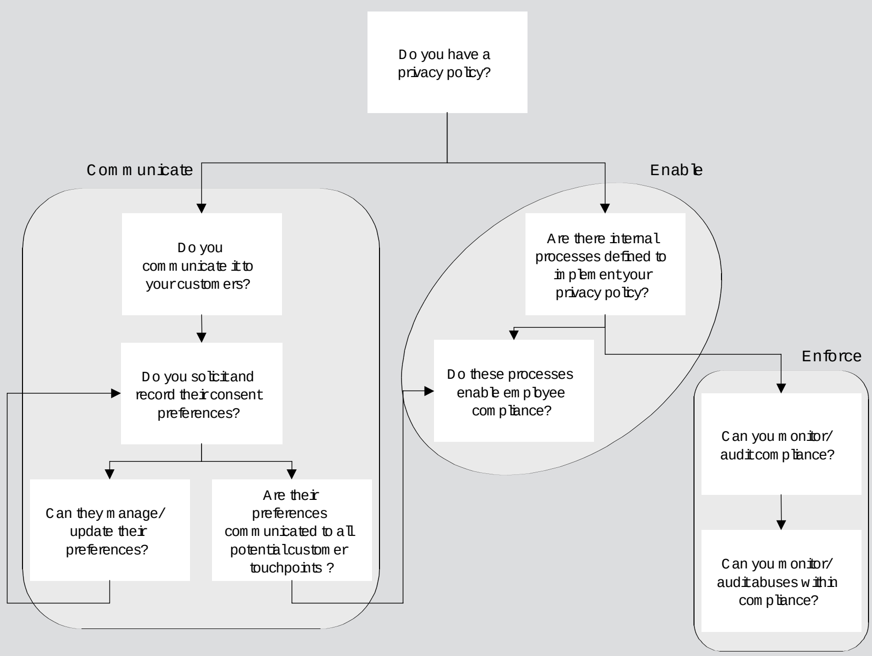
Do you solicit and record your customers' consent preferences? The two requirements in communicating your privacy policy to your customers are commonly known as notice and consent. Although making your privacy policy available to them provides notice of how you plan to handle their data, you must also solicit their consent to your intentions.

Whether your approach is to ask for opt-in (for example, "Here's what we plan to do, but only if you agree") or opt-out (for example, "Here's what we're going to do unless you tell us not to"), it is necessary to have a process in place to collect and retain customer responses indicating their preferences about how you handle their data. The more flexible your privacy policy and the more specific choices you provide for your customers, the more complex the process of collecting and maintaining these preferences will be.

Can your customers manage and update their consent preferences? A customer's privacy preferences are not static, and provisions must be made to allow for changes over time. A customer may grow weary of frequent bombardment with offers and choose to opt-out from future contact, or an interested customer may choose to opt-in to a new offering. Customers must have the ability to review the choices they have made in response to your privacy policy and be able to revise those choices as they please. Although this is commonly enabled via the company website, the process should be designed for the customer's convenience, and it should also be accessible by phone, by mail, in person or through whatever channel the customer prefers to use to communicate with the enterprise.

Are your customers' consent preferences communicated to all potential customer touchpoints? Once your customers' preferences are collected, how do you "spread the word"? Everywhere within the enterprise where there may be an opportunity for customer contact, those preferences must be accessible. When the customers express their preferences, they expect that it should only need to be done once. It is the

Privacy checklist



Source: Gartner Research (July 2003)

responsibility of the enterprise to collect those preferences wherever the customers might choose to present them, and to make sure that those preferences are communicated across the enterprise wherever a customer contact might occur.

ENABLE

Are there internal processes defined to implement your privacy policy throughout the enterprise? Processes must be in place to control the way customer data is handled within the enterprise once it is collected. The privacy policy explains what you need to do; the processes will dictate how you do it. An enterprise-wide memo that says "everyone must read the privacy policy and follow it" is not enough. A proper approach would be to perform a business process audit to identify every potential activity in which customer data is accessed and used. Then, assess each process to determine the appropriate controls to be put in place. In addition, if enterprise partners have access to any enterprise customer data, processes must be in place to ensure that they comply with the enterprise privacy policy as well.

Do these processes enable employee compliance? Once customer privacy processes have been established, employees should not need to make decisions about which customers they can access as prospects. When the internal distribution of customer information is managed by a central, higher-level role (for example, a senior manager or chief privacy officer), employees should only have permission, as dictated by that more senior level, to access names of customers who have granted contact permission.

> If an employee is overstepping his or her authority and abusing customer data outside the limitations of the privacy policy, can you detect it before the customer complaints start coming in?

Three Steps to Privacy Management

- Communicate customer privacy preferences to all necessary parties within your organisation.

- Enable access to customer data to senior level managers for appropriate distribution of data.

- Enforce privacy policies vigorously with stringent processes and monitoring technology.

ENFORCE

Can you monitor and audit compliance with your privacy policy? Your privacy policy is completed and communicated to your customers, you are collecting customer data and their consent preferences, your processes are in place, and your employees have been trained and educated. How can you be sure that everything is in place and running smoothly? There must be methods in place to ensure that all privacy communications are occurring smoothly, and that processes are being followed as defined. If an employee is overstepping his or her authority and abusing customer data outside the limitations of the privacy policy, can you detect it before the customer complaints start coming in?

If customers challenge that their data has been misused, can you prove that they were appropriately notified, that their preferences were collected, and that their data has only been accessed and used within the terms of your policy? An audit trail must be in place that records the details of all customer communications surrounding their consent preferences, along with data monitoring of who accessed the data, when, and for what purpose.

Can you monitor and audit abusive practices within the guidelines of your privacy policy? Even with appropriate compliance in place, it is still possible to abuse the privileges afforded by your privacy policy. For example, even though a customer may have opted-in to be contacted with offers about new products, that does not necessarily mean that he or she would appreciate receiving 20 new offers every day. Even within the definition of your privacy policy, there must be specific guidelines in place within the enterprise to control how customer information will be used, and you must be able to monitor and audit how those customer permissions are being used or abused.

BOTTOM LINE

When an enterprise is judging whether a particular business activity is effective, ethical or even legal from the perspective of customer privacy, the answer is simple. An enterprise can do anything it wants with a customer's data, as long as the customer has been informed of it and has consented to it. Although simple in concept, the processes and technologies required to communicate, enable and enforce that consent form a complex web of activities within an enterprise. To ensure total compliance with its privacy policy, an enterprise must effectively address all eight of the areas of the customer privacy management checklist.

i

AUTHOR: Walter Janowski is research director with Gartner's CRM Research practice and an IAPP member. He can be reached at: Tel: +1 203 316 1266, E-mail: bizapps@gartner.com.

This article first appeared in the *Privacy Officers Advisor* and is reprinted by permission of the International Association of Privacy Professionals, www.privacyassociation.org.

IMS Health: Raising staff awareness through e-training

PL&B International talks to **David Trower**, chief privacy officer for IMS Health, about the challenges of rolling out an e-training programme to the company's European employees.

E-training courses are increasingly being used by multinationals to raise staff awareness and can be an effective way to spread the data protection message across an organisation. But according to David Trower, rolling out a programme across a number of countries is more than just a case of bolting new software onto your corporate intranet.

IMS Health is a global provider of information to the health sector, collecting and analysing anonymised medical data which is utilised by health researchers, governments, pharmaceutical and biotec companies. Operating in a sector where the confidentiality of such sensitive data is paramount, provides organisations such as IMS with a strong incentive to implement high privacy standards, not just for the health information they process, but for client and employee data as well.

Strong internal procedures and policies are the bedrock of a good compliance regime, but at the end of the day they are nothing if not backed up with training to ensure that staff who process personal data understand their responsibilities.

Trower says that IMS decided to go ahead with an e-training programme after results from a data protection compliance audit indicated there was room for improvement on staff awareness of privacy issues.

But why choose e-training over the more traditional classroom-based awareness programmes?

"The traditional method has a certain inflexibility and dullness about it," explains Trower. "So we thought that a web-based course could be designed to be quite interactive and user-friendly, engender some interest, while at the same time be very flexible, in that people could do the course at their own leisure and new people, as part of their induction programme, could also do the course."

> "You can see the results when you speak to people who come for advice. They're clearly much more educated since they've done the course. I think it's been a real success."

One of the advantages of e-training, he says, is that it is much more visually stimulating than traditional training methods, where lawyers or consultants tend to come in and run through a slide show of data protection principles. Packages using graphics and animation avoid the 'boredom factor' while interactive elements that get staff to answer multiple choice questions or complete quizzes help to reinforce key privacy messages. Add to that mix the flexibility of a package that can be used anytime, anywhere and you have a programme that is ideal for large organisations trying to reach out to thousands of staff.

SETTING UP THE PROJECT

IMS' work on the project started at the end of 2002 with the plan to roll out the course to around 2,000 staff across seven European countries: the UK, France, Belgium, the Netherlands, Germany, Spain and Italy. To help manage the process, Trower appointed a project manager from the IMS legal team, as well as setting up a steering group comprising of representatives from IT, HR, legal and internal communications.

As the course was targeted at all staff from all levels across the organisation, the issue of where to pitch the content became a significant dilemma, he explains. Do you keep the course simple and straightforward, or do you include plenty of high level detail? "Ideally you want it at two levels," he explains, "with basic information for everyone, and then more detailed messages for key people, whether they be in security, marketing, or HR."

"In the end, you have to balance it against resources, and to have two versions of the course would largely have cost twice as much."

So instead, IMS decided to stick with one version of the course with the content pitched in the middle. "There's always a balance to be made," says Trower, "because we're a commercial organisation and we have to do things as cost effectively as possible."

TAILORING CONTENT

In developing the programme, IMS chose to partner with *Easy i*, a provider of interactive e-training programmes. One of the reasons for choosing the *Easy i* course, says Trower, was because it allowed them to adjust and tailor the content to make it more relevant to their staff. "We took the *Word* version of the course and customised it for our own company," he explains. "So we looked at the particular issues that are relevant to us, whether it be market research, the anonymisation issues that we have, or data transfers."

Flexibility was also required to roll out the course across different countries. Aside from the obvious language differences, the content of the training package had to be adapted to reflect variations in national laws. Trower explains that they started off with a master version of the course for the UK, and then used in-house counsel and external lawyers to adapt the master copy to address local variations such as response times to subject access requests, or definitions of data protection terminology such as what is 'personal data' or what is a 'data controller/processor'. They also tailored the 'enforcement' section of the course to add on country-specific examples of privacy breaches.

Once the legal side was completed, the content was then professionally translated into the correct languages and sent back to *Easy i* to make the software changes and carry out testing.

ROLLING OUT THE PROGRAMME

In delivering the course to staff, says Trower, input from the internal communications team was vital. "Clearly, one of the most important things was the communication about the rollout of the course, because you can't just dump it on people's laptops." The process involved a communication from the European President at IMS to reinforce the importance of the programme, in addition to keeping departmental line managers in the loop and explaining to them how the programme would be run.

Before launching the course to staff, they also carried out a final testing stage in each country. "We tested it on a few guinea pigs, both to see whether they could follow the course in terms of the content - whether it was too hard - and also in terms of whether the software was working."

ASSESSING THE RESULTS

One of benefits of most e-training programmes is that they enable companies to gain greater feedback into whether the programme has worked. Management reporting tools help the administrators to not only find out who has done the course, but how well they performed.

Trower stresses that although IMS monitored staff performance, the course was not designed to catch people out. There were no disciplinary procedures for failing the course, he explains. "It's simply an interactive and cooperative process. If we find that people keep failing, we'll go back and provide assistance and additional support."

Aside from one or two minor technical glitches, Trower says the course went extremely well, with an excellent response from employees. "I haven't had any negative feedback at all. People have said they found the course really interactive."

He has also seen a noticeable difference in staff awareness. "You can see the results when you speak to people who come for advice," he says. "They're clearly much more educated since they've done the course. I think it's been a real success."

Overall Trower says e-training is both a flexible and effective way to raise staff awareness. But, he warns that companies thinking of adopting similar programmes should bear in mind that things can often take longer than you expect. IMS set itself an ambitious timeframe, rolling out the programme on a consecutive country-by-country basis in under a year. "I think that if we were to do it again," he says, "we would do it slower. You have to be realistic about the amount of time you give to it. Because it is quite a complex process - in terms of the number of countries dealing with difficult issues, and the complexity on the IT side."

i

E-TRAINING: For details about *Easy i*'s data protection and privacy training programmes see www.easyi.com

Your Newsletter Subscription **Includes**

1. Five Newsletters a year
The *Privacy Laws & Business (PL&B)* International Newsletter, now in its 17th year, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from 50 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or e-mail us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. E-mail updates
We will keep you informed of the latest developments.

4. Index
Subscribers receive annually a cumulative Country, Subject and Company index. Multiple headings include advertising, data security, Internet, police, trans-border data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

e-Newsletter

Electronic Option
The newsletter is available, for an additional site license fee, in PDF format for uploading onto your Intranet or network. This format enables you to see the Newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in over 20 countries, including two thirds of the Financial Times UK Top 50 and half of the Fortune Top 20 global companies.

Privacy Laws & Business also publishes the United Kingdom Newsletter, a publication, which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.

Newsletter Subscription Form

❑ Send me a FREE sample of the *PL&B UK/International*

❑ Subscribe to *PL&B International* (£325/$600/€475)

❑ Subscribe to both International and UK newsletters (£520/$950/€750 or an extra £270/$490/€385 for existing UK subscribers)

Multiple subscription discounts:
❑ 2-9 copies - 30% discount
(please indicate number of copies..................)

Intranet site license (including up to 10 printed copies):
❑ *PL&B UK* (£1,250/$2,300/€1,825)
❑ *PL&B International* (£1,625/$3,000/€2,375)
❑ Both International and UK newsletters (£2,600/$4,750/€3,750)

❑ Print ❑ PDF (please tick preferred delivery format)
❑ I wish to receive PL&B's FREE e-mail news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ E-mail ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

E-mail:

Signature:

Date:

Payment Options

1. Cheque payable to *Privacy Laws & Business*

2. Bank transfer direct to our account:
S. H. Dresner T/A Privacy Laws & Business,
Barclays Bank PLC, 355 Station Road,
Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664

3. Credit card:
❑ American Express ❑ MasterCard ❑ Visa
(please indicate card and add an extra 3.75% for card charges).

Credit Card Number:

Name on Card: Expiry Date:

4. Please invoice me ❑

(Address of Credit Card/Accounts Dept if different):

Address:

Postcode: Country:

I am interested in:
❑ Consultancy/Audits
❑ In-House Presentations/Training
❑ Recruitment Service

Please return to: Newsletter Subscriptions Department, Privacy Laws & Business, 5th Floor, Raebarn House, 100 Northolt Road, Harrow, Middx HA2 0BX, UK Tel: +44 20 8423 1300
Fax: +44 (0)20 8423 4536 e-mail: sales@privacylaws.com 20/04/04

www.privacylaws.com

Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.