INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

India plans EU-style data law

A new law modelled on the EU Data Protection Directive could provide some regulatory relief for multinationals outsourcing their processing operations to India. **Alan Pedersen** reports.

The Indian government is preparing a new data protection law that could be introduced within the year, according to recent reports. Speaking at an IT strategy summit in Bangalore on June 12th, Rajeera Ratna Shah, federal secretary for the Department of Information Technology, said: "We are ready with the draft of the Data Protection Act. It might be possible to enact it in the winter session of Parliament."

Unlike government-led initiatives in other countries, the proposed law has received strong backing from business representatives. Kiran Kirk, president of the National Association for Software Service Companies (NASSCOM), expressed support for the proposals by highlighting the commercial benefits of introducing privacy legislation. "As we expand our global reach, some companies will insist on such a law before outsourcing work to India," he said. Rajeera Ratna Shah added that the "Data Protection Act will help in building confidence of foreign customers to outsource back-office work to third party vendors in India."

In addition to a new privacy law, Shah said that the government also plans to bolster data protection by setting up a cyber security assurance framework. Despite some business fears over data security, Stephanie Moore, senior analyst at Forrester research, says Indian firms have an "excellent reputation on security. Not only are they very conscious about making sure their physical processes are in place…they are also encrypting data and implementing clean desk policies."

The outsourcing industry in India has flourished over the last few years with multinational companies taking advantage of cheap, good quality labour to drive down operational costs. Research from IDC predicts HR outsourcing revenues will reach $15 billion by 2006. And according to Stephanie Moore, call centre outsourcing is becoming a booming industry with a growth rate in the region of 150 per cent year-on-year. "A lot of companies are looking to Indian vendors to provide them with call centres," she says.

> Unlike government-led initiatives in other countries, the proposed law has received strong backing from business representatives.

Aside from outsourcing, companies are also setting up their own subsidiary branches to handle call centre work, payroll processing and market research activities. The UK's *Financial Times*, for example, recently reported plans by British insurance company Prudential to save £16 million (€22.3 million) a year by shifting around a third of its customer service operations to a wholly-owned call centre in Bombay.

Continued on p.3

Issue 68 **May/June 2003**

NEWS & ANALYSIS

REGULATION

WORKPLACE PRIVACY

MANAGEMENT

INTERNATIONAL newsletter

ISSUE NO 68 May/June 2003

EDITOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

ASSOCIATE EDITOR
Eugene Oscapella
eugene@privacylaws.com

NEWS EDITOR
Alan Pedersen
alan@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Shelley Roche
shelley.roche@privacylaws.com

ISSUE 68 CONTRIBUTORS

William B Baker
Wiley Rein & Fielding

David E Case & Yuji Ogiwara
White & Case

Carol Leland
A&L Goodbody

Kate Brimsted
Herbert Smith

Laura Linkomies
Privacy Laws & Business

Nancy E Muenchinger
Denton Salès Vincent & Thomas

Vanessa Smith Holburn
Freelance Journalist

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

The *Privacy Laws & Business* International Newsletter is produced five times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. While every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

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

ISSN 0953-6795

comment

Flexing consumer muscles in the name of privacy

Consumers in many western nations rely on government-made rules to limit intrusions by sometimes over eager private sector organisations. But what can consumers do when there are no rules, or when the rules fail to protect, or are perceived to be failing? Worse yet, what can consumers do when governments themselves are involved in the plunder of personal information, encouraging or compelling private sector organisations to act as their agents?

Privacy advocates have long argued that good privacy policies and practices mean good business. Consumers, they maintain, will stay away from those organisations that do not respect privacy. That is, consumers may individually boycott businesses that do not respect their privacy.

Two stories in this issue of *PL&B International* highlight the next step in the evolution of the boycott. The personal boycott ("I won't shop there anymore") is evolving into the potentially much more powerful organised boycott ("Here's what this company is doing to your privacy. Let's all show our disapproval by boycotting the company").

We discuss the actions of one Texas businessman, angered by the collaboration between a US air carrier and the US government in collecting personal data (p.11). The strongest action that individuals can take to assert their privacy rights, he said, may be to withhold their custom. But his actions went beyond a simple personal boycott. He launched a website campaign which received over six million "hits" within two months.

The impact of organised boycotts may be difficult to measure, but the prospect of six million "hits" at a website discouraging individuals from dealing with a business is surely enough to make anyone take notice - and perhaps rethink their approach to privacy issues.

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 by E-mail: alan@privacylaws.com.

India privacy law, continued from p.1

EU-US THREAT

Despite phenomenal growth rates, Indian vendors are facing threats to their livelihoods. US attempts to resuscitate its flagging IT sector has led to the introduction of a number of state bills which aim to restrict outsourcing to developing countries like India. But NASSCOM believes that EU restrictions on data transfers pose a greater obstacle, and appear to be the reason why India is choosing to model its proposed law on the EU directive. Speaking to India's *Financial Express* in May, Kiran Karnik said: "This Act will take into consideration the minimum requirements set by the European Union…The threat from [the] EU is greater than it is from the US, and this Act will help us retain our position in the EU markets."

Companies locating their processing operations in developing countries are not having an easy time, says Suzanne Innes-Stubb, a lawyer at White & Case. "The current EU law makes it very difficult for multinationals to transfer data around the world, because if there isn't an adequacy finding by the European Commission, then they have to find a different solution."

The problem, she adds, is that there are a whole host of complex solutions depending upon the type of transfer taking place. "There isn't a standard approach that businesses are taking. You find some that are going for [the European Commission's] standard contractual clauses, while others prefer to have a more individualised approach - but that doesn't necessarily seem to be acceptable with all EU member states."

Daniel Cooper, attorney at Covington & Burling, says that businesses using the standard clauses have had mixed results, and for some it has been an unhappy experience. "There are some elements there that any business would be uncomfortable with," he says. "It increases your level of exposure to third party claims in particular, whereas an ordinary contract really doesn't have that effect because you don't give people third party rights to enforce their terms."

The problem with non-standard contracts is that companies could be exposing themselves to legal action should the contract fail to meet national privacy standards. This is a problem compounded by the fact that divergences between EU member states' approach to international transfers is creating an uneven playing field for businesses. "Some jurisdictions are more industry-friendly on data transfers," says Cooper. "Take for instance the UK where you are pretty much, as an organisation, allowed to make that [adequacy] assessment yourself." Then there is Spain, which takes a much tougher line, requiring prior authorisation before allowing data transfers to developing countries (see p.20).

But despite potential legal pitfalls over non-standard contracts, Cooper says that many businesses have "decided that the risk of their contact being determined to be inadequate is one they are going to take in order to facilitate the transfer."

> "The threat from [the] EU is greater than it is from the US, and this Act will help us retain our position in the EU markets."
>
> **Kiran Kirk, president, NASSCOM**

FINDING ADEQUACY

The solution to multinationals' problems would be for India to get an 'adequacy finding' from the European Commission. This would stimulate more trade with India by removing restrictions placed on data imports into the country.

The question is, though, if India does seek an adequacy finding, how long is it likely to take? To date, only four countries have been deemed by the Commission to be providing an adequate level of privacy protection - eg. Switzerland, Hungary, Canada (but only companies subject to the federal law) and the US (for companies signed up to the Safe Harbor scheme).

Unfortunately, getting an adequacy decision from the Commission is not a quick process. Despite the fact that the EU Data Protection Working Party published a favourable assessment of Argentina's privacy law in October last year, eight months on it is yet to be given formal approval. However, the Commission has recently indicated that Argentina could be granted adequacy within a matter of weeks.

Stewart Dresner, chief executive of *Privacy Laws & Business* who has worked with the Commission on adequacy reports, says few countries have been granted adequacy "because the European Commission does not have the resources to deal with many countries at once." He adds that it is a time-consuming process, requiring initial research by the Commission, reports from outside consultants, an opinion from the Working Party, possible amendments to the legislation being assessed, and final approval from the EU Article 31 Committee (a group made up of representatives from EU member states).

If India does seek an adequacy finding, it will have to join the back of a fairly substantial queue of countries, including Guernsey, the Isle of Man, Australia, New Zealand, Japan, and South Korea. And with the process generally taking around 18 months, even if India does manage to push its law through before the New Year, it will be mid-2005 at the earliest before a finding comes through.

India may also have to battle for position with other countries pushing for an adequacy finding, but its strong trading ties with Europe could work to its advantage and push it higher up the Commission's agenda.

Even without an adequacy finding, Daniel Cooper says a new privacy law represents a step in the right direction for India and a boost for multinationals. "The ideal situation would be a law that would provide adequate protection in the eyes of the European Commission," he says. "But even short of that, having an effective data protection law would certainly go a long way to easing some of the fears of European regulators that once data is transferred out of the EU, effective control of that data might be lost."

WEB LINKS: India's Department for Information Technology: www.mit.gov.in

The National Association for Software Service Companies (NASSCOM): www.nasscom.org

global privacy roundup

ARGENTINA

A criminal investigation has been launched over the sale of personal data to US list broker, Choicepoint. The company has been buying personal data taken from public sector databases across a number of Latin American countries (including Argentina, Mexico, Columbia, and Costa Rica) and selling it on to government agencies in the US. The investigation was launched after a complaint from Argentina's Data Protection Commissioner who argued that the sale breached the country's data protection law. According to the *Associated Press*, similar investigations are being initiated in Mexico and Costa Rica.

AUSTRALIA

According to *Computerworld*, Federal Privacy Commissioner Malcolm Crompton is to investigate the transfer of airline passenger details to law enforcement agencies in the US. Crompton stated that the issue was "sufficiently serious to warrant investigation" stating that it was unclear how much personal data is being disclosed to US agencies and what privacy safeguards they have in place.

BELGIUM

The Belgian Data Protection Commissioner is to investigate whether airline carriers, Continental Airlines and United Airlines, breached the country's data protection law by transferring passenger details to government agencies in the US. The investigation was initiated after lobbying from pro-privacy group, European Digital Rights, and MEP Marco Cappato of the Transnational Radical Party.

CANADA

A new bill (The Personal Information Protection Act) aimed at regulating private sector organisations was introduced into the British Columbia legislature on April 30th. If approved, the law could come into force by January 1st next year. Canada's Federal Privacy Commissioner, George Radwanski, has criticised the bill, saying it contains "grave deficiencies". He has also made similar comments over the private sector privacy bill being proposed in Alberta.

Meanwhile, the Privacy Commissioner for British Columbia has published his annual report for 2002-03. For a copy of the report and further information on the Personal Information Protection Act, see the Commissioner's website at: www.oipcbc.org

DENMARK

In May, software company, Fonn Danmark, was fined 15,000 kroner (€2,021) for sending unsolicited advertising. According to the *Associated Press*, the Maritime and Commercial Court in Copenhagen found that Fonn Danmark had breached the Danish Marketing Practices Act which states that electronic communications cannot be sent without prior consent. Although the company reportedly sent out only 156 "electronic advertisements", Denmark's Consumer Agency decided to take legal action after receiving 50 complaints from consumers.

EUROPEAN UNION

The European Commission has published the findings from its first review of the EU Data Protection Directive. Conclusions are that the directive has been successful, although the lack of harmonisation between member states' laws has prevented the directive from fully achieving its goal of consumer protection and facilitating the transfer of data around the EU. See p.22 for full report.

The EU Article 29 Data Protection Working Party has published two new documents. The first relates to the use of binding corporate rules for international data transfers (see p.8). The second covers data protection issues in e-government.

Stefano Rodota, chairman of the EU Article 29 Data Protection Working Party, has stressed the need for a global approach to the e-mail spam epidemic. Although the EU E-Communications Privacy Directive places restrictions on unsolicited e-mailing within Europe, businesses and individuals have no legal redress against foreign spammers. Speaking to *Reuters* last month, Rodota said: "US companies are reacting by filing lawsuits asking for massive compensation. But for EU firms it is more complex to defend themselves against US spam. We need an international convention or common rules."

FRANCE

France's Data Protection Authority (CNIL) has welcomed the French Banking Federation's approach to providing data protection information to bank customers. Financial regulations (the MURCEF law) passed in December 2001 require banks to provide customers with written contracts before opening accounts. Although the regulations do not come into force until 2004, the CNIL has welcomed the Federation's proactive response to the issue of drafting data protection information into the contracts.

Some banks have already drafted contracts, providing customers with information on processing for credit reference purposes, whether personal data is shared with third parties, the right to opt-out from marketing contact, as well as subject access rights.

GREECE

The success of a new credit rating system is in doubt after objections from the Greek Data Protection Authority. The 'Teiresias' credit rating system aims to

boost the flagging Greek credit industry by allowing banks to share client data.

The country's data protection law, however, requires banks to gain consent from customers before putting their details onto the central Teiresias system. Proposals to bypass this consent provision by informing customers through adverts in the press have been rejected by the Data Protection Authority.

HUNGARY

According to law firm Baker & McKenzie, a draft amendment to Hungary's Data Protection Act could significantly enhance the Data Protection Commissioner's powers. The amendment, which is being prepared by the Minister for Justice, would give the Commissioner greater powers to investigate compliance by public and private sector organisations. Sanctions could include ordering the deletion of personal data, and enforcing changes to data processing procedures.

IRELAND

On April 10th, the Irish government passed amendments to the existing Data Protection Act, bringing the country in line with the EU Data Protection directive. The law comes into effect on July 1st. See p.18.

ITALY

The Italian Data Protection Authority (IDPA) has published its annual report for 2002. See p.9 for more details.

Following an investigation into unsolicited e-mailing (see *PL&B International*, March/April, p.4), the IDPA has taken action against seven companies for illegally collecting e-mail addresses and using them for advertising purposes. The companies have been prohibited from the practice while the IDPA carries out a full investigation.

JAPAN

On May 23rd, Japan's Upper House approved five privacy protection bills which will regulate data protection across both the private and public sectors. Penalties for breaching the new privacy law include fines of up to 300,000 yen (around €2,200) and a six month prison sentence. See p.15.

The government is to launch an investigation into alleged privacy breaches by the Organisation for Pharmaceutical Safety and Research. The organisation, which helps patients suffering side-effects from prescription drugs, reportedly disclosed their details to the institutions that prescribed the drugs. According to the *Japan Times*, the details (including name, age, sex, and medical data) of around 3,400 people have been disclosed without consent.

NETHERLANDS

The Dutch Lower House has approved changes to the Telecommunications Law that will give all law enforcement agencies access to customer records held by communications service providers. Access has previously been restricted to 500 public prosecutors and the secret service. The changes will also allow public prosecutors to access data without the need for prior judicial approval.

According to *Europemedia.net* the Dutch Cabinet has agreed to a request by the Home Affairs Office to allow certain government agencies (for example, the Centre for Work and Income, and the police) access to personal data held by local public sector bodies.

SOUTH AFRICA

According to *Business Today*, the South African government is to propose legislation that will allow private sector organisations to use the national population registry (electoral roll) for business and marketing purposes.

A survey carried out by Ernst & Young has shown that 89 per cent of the 800 South Africans questioned support the introduction of new privacy legislation. 90 per cent were concerned about companies passing their details on to other businesses without their consent. 96 per cent would ask for their details to be deleted if their information were misused.

UNITED KINGDOM

The Information Commissioner's Office has published the third part of its code of practice on workplace privacy. The third section deals specifically with monitoring and surveillance, providing guidance on issues such as staff use of e-mail and the Internet, and use of CCTV cameras for covert surveillance. The two previous sections of the code covered recruitment and selection, and handling employment records. The final section, dealing with medical testing in the workplace, is expected to be published later this year. See p.10

The UK Direct Marketing Association (DMA) has voiced its opposition to plans by the Department of Trade & Industry (DTI) to allow businesses to register with the Telephone Preference Service. The proposals form part of the DTI's draft regulations implementing the EU E-communications Privacy Directive. In a statement, the DMA said the plans would have a "devastating impact on business-to-business marketing" and hit the SME sector particularly hard.

A UK citizen, James Hewitson, has been awarded €4,800 by the European Court of Human Rights after it held that the police had violated his right to privacy under Article 8 of the European Convention on Human Rights (ECHR).

The *Hewitson vs the United Kingdom* case involved the police placing a listening device on Hewitson's property in 1995. The Court held that because there was no law regulating covert monitoring at the time, the police's actions were not in accordance with the law and therefore a violation of Article 8 of the ECHR. See www.echr.coe.int for the full judgment.

UNITED STATES

On July 1st, a new privacy law will be introduced in the US state of California that will require businesses to inform customers of any security incidents in which their personal data is stolen. According to newswire *Computerworld*, lawyers have warned that many businesses are unprepared for the new regulations and could be exposed to costly lawsuits.

Amazon accused of child privacy violations

Towards the end of April, US consumer groups petitioned the Federal Trade Commission (FTC) to investigate alleged breaches of the Children's Online Privacy Protection Act (COPPA) by online retailer Amazon. The COPPA law applies to any online businesses targeted at children, or knowingly collecting information from them. Businesses are required to post privacy policies, get verifiable parental consent when collecting data from under-13s, allow parents to access their children's details and block any further processing.

Already this year, there has been significant enforcement action taken against child-orientated sites. In February, the FTC imposed record penalties on Mrs Fields Cookies and Hershey Foods ($100,000 and $80,000 respectively) for COPPA violations (*PL&B International*, March/April 2003, p.16).

Although Amazon sells children's toys through its website, it claims that it is not required to comply with COPPA as it does not market products at children. The company's privacy policy states: "Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian."

However, consumer groups (including the Electronic Privacy Information Centre, the Centre for Media Education, and Junkbusters) argue that Amazon falls under the scope of COPPA on two counts. Firstly, they state that the "Toy Store" section of Amazon's website is clearly targeting children. Secondly, they allege that Amazon is knowingly collecting children's details through its product review section. Children and adults are able to post reviews of games, books, music etc. on Amazon's website after registering their details. Although Amazon's site does have a separate "Kid's Review Form", allowing children to post anonymous reviews, consumer groups claim that the hyperlink to the form was often not working, forcing children to posted reviews via the adult section [Amazon has since announced that it has fixed the link].

Consumer groups claim a statement by Amazon that it screens product reviews is proof that the company is knowingly collecting information from under-13s. It cites cases in which childrens' names, ages, gender, e-mail and postal addresses have been posted online.

In response to the accusations over Amazon's privacy practices, the FTC stated that it will look into the consumer groups' claims, but has not confirmed whether it intends to launch a formal investigation. Amazon has continued to deny that it needs to comply with the COPPA regulations. A spokesperson for the company told the *Washington Post*: "We are not a site that's directed at children. We're a store. We sell things, and you need a credit card to buy them. When it comes to reviews, we created special software for anonymous reviews by children under 13."

New York hotel feels wrath of privacy activist

The management of one New York City hotel is tending its wounds after butting heads with a determined American privacy activist. To make matters worse for the management, a recounting of their security imbroglio, complete with an embarrassing audio file, is now posted on the Internet, along with a call by the activist for a worldwide boycott of the Ramada hotel chain.

Mike Stollenwerk of the Fairfax County Privacy Council had travelled to New York to attend the April 2003 Computers, Freedom and Privacy conference. He had made a credit card reservation for his hotel room. On his arrival late in the evening, he presented his credit card but was told he must present photo ID. Stollenwerk refused. After an hour of heated discussions with hotel staff, Stollenwerk presented his voter registration card (which had no photo). The receptionist photocopied these documents, and he was then allowed to go to his room (He was later told that the hotel would keep these photocopies for about 30 days).

The next day, Stollenwerk received a message asking him to meet with the hotel security director. At that meeting, citing legal precedents, Stollenwerk explained his objections to presenting photo ID and having it photocopied.

The tale did not end there. Returning to his room after the day's conference, Stollenwerk found the following message on his voicemail: "This is Barry Mann, General Manager of the hotel, Mr Stollenwerk. Ahhh, it's a little after nine in the morning. I'd like you to come down and present some picture ID. Otherwise, the next knock on the door will be the police terrorism squad. Thank you."

The police terrorism squad never did appear. And Stollenwerk had the presence of mind to consult with his conference colleagues and record the manager's message on a digital recording device. The audio file of the manager's message is now posted on the Internet.

Says Stollenwerk: "[N]ow I know why New York City is the 'city that never sleeps' - because you can't sleep in New York City hotels unless you have Photo-ID and let the hotel copy and retain it."

Report by Eugene Oscapella

The audio file containing the manager's "terrorism squad" warning, and Stollenwerk's diary of the encounter, can be found at: http://www.privacyrights.org/ar/NYRamada.htm

European e-tailers weak on privacy

A survey published in April by IT World Lawyers has revealed that online businesses in Europe are failing to comply with data protection legislation. The survey, carried out by IWD Market Research, looked at a total of 420 websites across seven countries which sell a range of products such as electronics, books, and holidays. It found that only around half of the websites studied contained some form of privacy policy or data protection statement.

Results showed that while the UK leads Europe in terms of transparency (71.7 per cent of UK sites posted a privacy policy), France lagged well behind with only 31.7 per cent bothering to communicate their privacy practices.

More worryingly, only a quarter of the 420 websites gave consumers the option to opt-out from direct marketing. Portugal topped the table in this category with 35.3 per cent providing an opt-out, while Germany and Spain bottomed-out at 18.3 per cent.

The survey also revealed non-compliance with other e-business legislation. Only 29.7 per cent, for example, complied with the EU Distance Selling Directive by informing consumers of their right to withdraw from a contract within seven days. Additionally, around 40 per cent failed to provide an electronically available version of their standard business terms.

The countries included in the survey were: France, Germany, the Netherlands, Portugal, Spain, Switzerland, and the UK.

Global businesses face tighter controls over data transfers

A new data protection survey has shown that global businesses face an increasingly complex set of obstacles when transferring data between countries. The 2003 Data Protection Survey, published by White & Case in conjunction with the law firm's Global Privacy Symposium last month, specifically looked at how divergences in privacy laws are preventing the free flow of information across borders.

The survey examined 22 key jurisdictions from Europe, the Asia-Pacific region, and North America (including four non-sovereign states - California and New York in the US, and Ontario and Quebec in Canada).

Key findings revealed that most of the jurisdictions surveyed place some degree of restriction on cross-border transfers and that the EU Data Protection Directive is emerging as a benchmark by which jurisdictions measure their data transfer procedures.

12 of the 22 jurisdictions surveyed place restrictions on data transfers with another five (Hong Kong, Malaysia, Mexico, Thailand, and Ontario) considering proposals to do so. But, the survey found discrepancies in the way these 12 jurisdictions handle cross-border data flows.

All 12, for example, allow the use of customer or employee consent to legitimise data transfers. However, nine operate an opt-in approach to consent, while Australia, the UK and Quebec allow consent to be gathered on an opt-out basis.

9 of the 12 jurisdictions surveyed allow data transfers in cases where it is necessary to protect the vital interests of the individuals concerned, but only four jurisdictions have approved a standard contract for cross-border transfers.

Robert L Raskopf, head of the IP and E-commerce, Media and Technology practice groups at White & Case, summed up the complexities facing businesses by using the example of data flows between Australia and Spain. An Australian-based business, he said, would be permitted to export personal data to Spain if it were necessary to protect individuals' vital interests, but transferring information from Spain to Australia under the same circumstances would not be allowed.

Similarly, while Spain would allow information to be transferred to Australia in the context of defending a legal claim, the reverse process would again be prohibited.

For a copy of the White & Case 2003 Data Protection Survey, see: www.whitecase.com

Jurisdictions surveyed were:

EUROPE	ASIA-PACIFIC	NORTH AMERICA
France*	Australia*	Mexico
Germany*	China	Canada*
Hungary*	Hong Kong	United States
Italy*	Japan	Ontario
Poland*	Malaysia	Quebec *
Russia*	South Korea*	California
Spain*	Thailand	New York
United Kingdom*		

(Jurisdictions which restrict cross-border data transfers)*

News in brief

CORPORATE PRIVACY

US Internet service provider, Verizon, is to hand over the names of four anonymous customers who have been accused by the Recording Industry Association of America (RIAA) of illegally swapping music files. On June 4th, the US Court of Appeals for the District of Columbia backed earlier judgments forcing Verizon to comply with disclosure subpoenas issued last year by the RIAA under the Digital Millenium Copyright Act.

Earthlink has been awarded $16.4 million (€14 million) in damages after a New York-based spammer sent 825 million spam e-mails through the US-based Internet service provider's servers. According to *NewsFactor.com*, Earthlink also won $25 million (€21 million) from a Tennessee-based spammer in 2001 - although it has yet to receive any payment.

According to the 2003 Global Security Survey published by Deloitte Touche Tohmatsu, consumer expectations play little part in organisations' decision to implement good privacy practice. While 90 per cent of respondents cited legal and industry regulations as a key driver for getting privacy compliant, only 47 per cent considered the privacy expectations from their customers to be an influencing factor.

IT analyst firm, Gartner, says US companies that fail to implement robust privacy practices risk customer backlash and could force the government into creating further privacy legislation. Walter Janowski, research director at Gartner, said: "In a climate in which the general public is greatly concerned with corporate ethics and accountability, a business that makes a significant misstep in managing its customers' private information could have a highly visible and damaging public scandal…If US businesses don't prioritise privacy management, public outcry will motivate the US Congress to mandate restrictive privacy legislation."

EU 'corporate rules' report published

On June 4th, the EU Article 29 Data Protection Working Party published a report on proposals to allow the use of 'binding corporate rules' for international data transfers. Multinational companies such as BP, Shell and Accenture are already trialing the scheme which aims to ease restrictions on data exports outside the EU (see *PL&B International*, March/April, p.1).

The Working Party proposals envisage organisations creating a single legally binding privacy policy that would then be approved by EU data protection authorities.

Conditions for authorising the use of the 'corporate rules' scheme would require companies to not only train their staff in data protection, but also demonstrate good levels of awareness within the company. The scheme would also require regular privacy audits supervised by external auditors. Companies would be required to submit the results to data protection authorities and act on any advice or recommendations given.

Companies would also have to set up proper complaints handling procedures, inform employees and customers of their privacy practices and details of international data transfers. Individuals would be able to take legal action, not only in their home country, but also in the country in which the company has located its headquarters (provided it is in the EU). Companies would be required to demonstrate that they have sufficient assets to cover any compensation that might arise as a result of a privacy breach.

The Working Party has stressed, however, that the corporate rules scheme will not necessarily be the correct approach for all organisations. "For loose conglomerates," says the report, "binding corporate rules are very unlikely to be a suitable tool." The Working Party also states the scheme "should not be considered as the only or the best tool for carrying out international transfers," but rather as an additional option in situations where other methods (such as the European Commission's standard contractual clauses) "seem to be particularly problematic."

For a copy of the Working Party's report, see: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

Ireland amends DP law

On April 10th, Ireland passed the Data Protection (Amendment) Act 2003. The changes have been incorporated into the existing 1988 Act. The amendments bring Ireland into line with the EU Data Protection Directive and come nearly five years after the deadline for transposing the directive - Ireland was in fact prosecuted in the European Court last year for the delay (*PL&B International*, June 2002, p.9).

The new amendments come into force on July 1st and include provisions on manual data, sensitive personal data, the use of public registers for marketing, and strengthened rights over access to data. A guidance document to help organisations comply with the new law has been published on the Data Protection Commissioner's website.

Meanwhile the Commissioner, Joe Meade, has published his annual report for 2002. Figures show that complaints are down nearly 20 per cent from 233 in 2001 to 189 last year. However, complaints are still significantly higher than the 131 received in 2000, and could rise again because of the Commissioner's plans to launch a public awareness campaign over the coming year.

The majority of complaints were against the financial services industry (24 per cent) and the telecoms sector (16 per cent). Most of the complaints that were lodged concerned access to personal data (30 per cent) and direct marketing (29 per cent).

See p.18 for more details on the Data Protection (Amendment) Act 2003.

Dutch DPA pledges support for industry codes of practice

According to its annual report for 2002, the Dutch Data Protection Authority (CBP) has made significant progress in promoting self-regulation among private sector organisations. During 2002 it formally approved the first industry code of practice for companies involved in pharmaceutical research. And, in January this year, a second code governing the financial sector was approved.

Three more codes - covering private investigators, court bailiffs and employment agencies - are expected to be approved this year. However, talks between the CBP and representatives from 'trade information agencies' (which process credit/debt information) for a code of practice have reportedly stalled. The CBP has labelled compliance within the sector as "thoroughly unsatisfactory" and has pledged to take a firmer line in the future. "The best solution," it says, "is likely to lie in further regulations on the way personal data is obtained for credit rating and debt collection purposes."

The CBP's report also details other efforts to promote self-regulation. Progress has been made in efforts to develop a data protection auditing scheme for organisations. In response to consultation with accreditation firms, the CBP has agreed upon a scheme for accrediting privacy auditors. Already, a number of organisations have agreed to act as accreditation bodies which will be responsible for approving privacy auditors. These auditors will then be empowered to issue organisations with certificates for good privacy compliance.

Along with efforts to promote good compliance, the CBP has also been stepping up its enforcement activities. During 2002 it set up a new department dealing specifically with complaints appeals, and created a new enforcement strategy. One of the initial target areas for enforcement is organisations which have not notified their processing operations with the CBP.

For a copy of the CBP's annual report see: www.cbpweb.nl

Italian privacy complaints are on the rise

Official complaints from individuals over violations of their privacy have risen nearly 60 per cent over the last year, according to the Italian Data Protection Authority. Figures published in its annual report show that there were 3,689 complaints in 2002 compared to 2,327 the year before. Additionally, the authority dealt with 12,800 requests for information on data protection issues.

Many of the complaints were focussed on unsolicited e-mail marketing. An investigation launched by the authority earlier this year revealed that many organisations were illegally collecting e-mail addresses by harvesting them from public areas of the Internet. The authority has stressed the need for a clearer legal framework on the use of personal data over the Internet.

The report revealed that the number of settled legal actions has more than doubled, from 211 in 2001 to 500 in 2002. Most cases, according to the authority, involved data protection breaches in the telecoms sector.

The authority has also stepped up its enforcement activities, doubling the number of official investigations to 40 in 2002.

A copy of the annual report for 2002 can be found at: www.garanteprivacy.it/garante/navig/jsp/index.jsp

Swedish e-tailers unaware of privacy rules

Swedish e-businesses have poor data protection knowledge, according to a report from the Swedish Data Protection Authority (DPA). The report, published in May, found that many companies are not familiar with even the most basic privacy principles.

The DPA investigated the privacy practices of 46 randomly chosen e-commerce companies after having received a number of complaints. The companies represented the travel, health and leisure sectors, and included well-known brand names such as IKEA and SAS.

Of those interviewed, only 12 identified themselves as data controllers. Information given to individuals about access and the purposes for which their data will be used was insufficient. Half of the respondents did not provide any information, and only two complied fully with the law's requirements in this respect.

All of the respondents used customer data for marketing purposes, and one third also forwarded address details on to business partners and other third parties. Rules on data security were generally not well known. Many of the respondents had not carried out any kind of risk assessment. Companies also lacked processes to destroy unnecessary personal data. Half of the respondents never destroyed any personal data. Some of those which destroyed unnecessary data only did so every six years.

The Swedish Data Protection Act requires data subjects' consent for the processing of sensitive data as well as, in most cases, for the processing of ID-numbers. One third of the respondents stored individuals' ID-numbers on their systems.

The DPA has published the findings (in Swedish) on its website www.datainspektionen.se, along with tips for e-commerce companies on how to comply with the Data Protection Act. The authority plans to carry out further compliance checks in the future.

Report by Laura Linkomies.

UK publishes workplace privacy code

On 11th June, the UK Information Commissioner published its long-awaited code of practice on employee monitoring. The code is the third in a four-part series dealing with a variety of data protection issues in the workplace.

While it is not legally binding, there are fears that employment tribunals could refer to the code when making their judgments.

The code applies to a number of potentially invasive practices including monitoring e-mail and Internet use, CCTV/video surveillance, vehicle tracking technologies, and using third parties such as private detectives to monitor employees.

Key guidance in the code includes creating 'impact assessments' to judge whether monitoring is necessary, delegating monitoring responsibility to trained staff, promoting staff awareness of monitoring practices, and avoiding snooping into workers' personal correspondence.

Information Commissioner, Richard Thomas, commented: "If any monitoring is to take place, it must be open and transparent and with the knowledge of the employee. In reality there are few circumstances in which covert monitoring is justified."

A copy of the "Monitoring at Work" code is available from the Information Commissioner's website: www.dataprotection.gov.uk/dpr/dpdoc.nsf.

The final section of the workplace privacy code, covering medical testing and health data is expected to be published at the end of this year.

events diary

Privacy Laws & Business 16th Annual International Conference - Transforming Risk Assessment Into Everyday Compliance with Data Protection Law
July 7-9, Cambridge
This year's event features 46 speakers from 7 countries, including the regulatory authorities from the United Kingdom, the Netherlands and Hong Kong, in addition to a host of sessions on a wide range of both data protection and freedom of information issues.
Contact: Shelley Roche, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: shelley.roche@privacylaws.com
Website: www.privacylaws.com

The Body As Data
September 8, Melbourne, Australia
A one-day conference featuring a keynote address from Stefano Rodota, head of the Italian Data Protection Authority and chairman of the EU Data Protection Working Party. Presentations cover privacy implications on issues such as genetics and biometrics.
Contact: Office of the Victorian Privacy Commissioner
Tel: +61 3 8619 8719
Fax: +61 3 8619 8700
E-mail: conference@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Global Privacy Management
September 9, Sydney, Australia
A one-day conference intended to provide an opportunity to learn and share in the latest developments in privacy implementation across the world.
Contact: Tim Dixon, Australian Corporate Privacy Officers' Network
Tel: +61 2 9225 1564
E-mail: mail@cpo.net.au
Website: www.cpo2003.com

25th International Conference of Privacy and Data Protection Commissioners
September 10-12, Sydney, Australia
The theme for this year's annual conference is 'Practical privacy for people, government and business' and features presentations from privacy commissioners and representatives from the public and private sectors and other interested groups.
Contact: Tour Hosts Conference & Exhibition Organisers
Tel: +61 2 9248 0800
Fax: +61 2 9248 0894
E-mail: privacy2003@tourhosts.com.au
Website: www.privacyconference2003.org

The Data Protection Act Explained - Basic Training for Beginners
September 24 - London; October 29 - Bristol; November 26 - Edinburgh; December 17 - London
Privacy Laws & Business consultant, Sandra Kelman, presents a series of training workshops aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act.
Contact: Sandra Kelman, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: sandra@privacylaws.com
www.privacylaws.com/whats-newframe.htm

How to use the Information Commissioner's Data Protection Audit Manual
July 8-9 - Cambridge; September 15-16 - London
Privacy Laws & Business is conducting a series of two day interactive audit workshops across the UK or in-house.
Contact: Shelley Malhotra, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: shelley@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

Delta Airlines suffers privacy boycott

Eugene Oscapella finds that consumers are starting to challenge corporate privacy intrusions by hitting them where it hurts - sales revenues.

The consumer purse is a powerful incentive for companies to respect privacy. One vehicle for flexing the muscle of that purse - the consumer boycott - is being tested on an American air carrier, Delta Airlines, at a time when the airline industry is already on its knees because of weak travel demand.

Bill Scannell, a software executive based in Austin, Texas, began a boycott campaign through his "boycottdelta.org" website in March. His call for a boycott may give many companies good reason to reflect on their privacy practices.

In a recent interview with *PL&B International*, Scannell explained the simplicity of his quest - to be able to travel freely in the United States without having to confront internal border controls. Scannell's immediate concern arose over the cooperation between Delta Airlines and the US Transportation Security Administration on a passenger screening programme. Delta Airlines agreed to test the US CAPPS-II programme, a travellers' profiling system that intends to use extensive data mining of credit history, criminal records, and travel patterns, among other sources of information, to profile all airline passengers.

According to Scannell, Delta began running intrusive background checks in March on anyone who flies Delta from one of three undisclosed airports. These involved credit, banking history and criminal background checks.

Scannell explained to *PL&B International* that if governments do not respond to the privacy concerns of their citizens, the appropriate response may be to "follow the money trail" to the businesses that are cooperating with governments in undertaking intrusive behaviours. In other words, the strongest action that individuals can take to assert their privacy rights may be to withhold their custom from these businesses. It is difficult to take on a government, argues Scannell, but consumers can always use their collective financial might to encourage more responsible corporate behaviour.

Boycotts can have another benefit, he notes. Many groups have written papers about profiling systems such as that being used by Delta. However, most have failed to get the attention of the media or correct the offending conduct. His "Boycott Delta" programme, on the other hand, resulted in extensive coverage on *CNN* and in major media such as the *New York Times*.

> the strongest action that individuals can take to assert their privacy rights may be to withhold their custom

Scannell said that he stopped keeping statistics on visits to his "boycottdelta.org" website in late April, by which time the site had received over six million "hits". By the start of June, he had received 8,900 e-mails on the issue.

FURTHER INFORMATION: For details on the Delta Airlines boycott, see: www.boycottdelta.org

News in brief

SECURITY

A security flaw in Microsoft's Net.Passport authentication service could have exposed the accounts of around 200 million users, according to IT analysts, Gartner. Microsoft has said that it fixed the flaw within eight hours of discovery. However, according to *NewsFactor.com*, the Federal Trade Commission (FTC) may investigate whether the flaw violated the terms of a privacy settlement reached last year between Microsoft and the FTC (see *PL&B International*, September 2002, p.15).

Staff at UK broadcaster, the BBC, are being advised not to use a new internal intranet system set up for registering conflicts of interest. According to *the Guardian*, broadcasting unions are concerned that allegedly lax security controls could leave employee data exposed and the BBC in breach of the Data Protection Act. It is claimed that anyone who knows an employee's name and staff number could gain access to their records. A spokesperson for the BBC has denied that the system breaches the Data Protection Act.

A survey of 500 US workers dealing with customer information has revealed that 66 per cent believe their colleagues present the greatest threat to customer privacy. According to the survey, conducted by Harris Interactive (on behalf of IT security firm Vontu), nearly 70 per cent of respondents said their company had policies regulating the disclosure of personal data. Yet, around 80 per cent said they had not read it. 45 per cent said that it would be easy for a colleague to remove sensitive customer data from the corporate network.

News in brief

ONLINE PRIVACY

On 28th May, the Committee of Ministers of the Council of Europe adopted a declaration on freedom of communication on the Internet. The purpose behind the declaration is to strike a balance between freedom of expression and other rights under the European Convention of Human Rights, such as the Article 8 right to privacy. For the full text of the declaration: www.coe.int

A group of scientists has warned a US House of Representatives Government Reform Committee over the privacy dangers of peer-to-peer file sharing. Programmes such as Kazaa and Morpheus allow users (often employees) to link up their computers and share files online. But scientists have said that failure to properly set up the programmes could leave confidential information such as e-mail, legal documents and password lists, open to outsiders.

The US Direct Marketing Association has condemned the so-called practices of e-mail 'harvesting' and 'dictionary attacks' which are used by spam merchants to compile vast marketing lists for unsolicited advertising. Such practices, says the DMA, constitute abuses of the right to send e-mail legitimately and could impact upon the use of e-mail as a key business communications tool.

The DMA has warned its members to abide by its four pillars of reputable e-mail marketing: (1) honest subject lines (2) accurate header information that has not been forged (3) include physical contact addresses for consumer redress (4) an opt-out that works.

According to e-mail solutions provider, MessageLabs, one in three e-mails is now unsolicited spam advertising. In March this year, MessageLabs analysed 104.9 million e-mails, discovering that 38.1 million were spam. Additional research found that nearly 60 per cent of spam originates from the US.

Unauthorised cookies could violate US federal wiretap law

A recent US Court of Appeals decision provides valuable insight into the legal implications of collecting personal data through web cookies. By **William B Baker**

The US Court of Appeals for the First Circuit ruled on May 9th that a web services company may have violated the Electronic Communications Privacy Act (ECPA) by collecting personal information about consumers without the consent of the websites which the consumers were visiting. The decision, in *In re Pharmatrak, Inc. Privacy Litigation*, 2003 WL 21038761 (1st Cir. 2003), marks an important interpretation of ECPA and has broad implications for the use of third-party cookies in collecting information about individuals who visit Internet websites.

PHARMATRAK'S SERVICE

The Pharmatrak litigation arose from an arrangement by which Pharmatrak provided website monitoring services for a number of pharmaceutical companies. The Pharmatrak service collected information about visitors to the client companies' websites that would be used for intra-industry comparisons of website traffic and usage. For example, Pharmatrak would track whether visitors were first-time or repeat visitors, the "referrer pages" from which they came and similar information. Important to the Court's decision was evidence that the pharmaceutical companies did not want Pharmatrak to collect personal or identifying data about their site visitors.

Pharmatrak provided its service, called "NETcompare", through the use of a "web bug" or "clear GIF"—a tiny graphical image not noticeable by the casual user. HTML code in the pharmaceutical company website would retrieve the web bug from the Pharmatrak server, and Pharmatrak would place a cookie on the user's computer.

Although Pharmatrak denied any intent to collect personal information, several configurations of website usage in fact allowed Pharmatrak to collect personal information about a small number of users of certain sites. In discovery, plaintiffs' expert was able to find detailed user profiles of 232 users on Pharmatrak's servers (Pharmatrak set some 18.7 million cookies during the relevant period).

In their class-action complaint, plaintiffs sued both Pharmatrak and the pharmaceutical companies, declaring that the arrangement violated a number of federal and state privacy laws, including Titles I and II of ECPA, the Computer Fraud and Abuse Act and several Massachusetts statutory and common laws. The US District Court granted summary judgment to defendants on these claims. (See "Light Shining on Web Beacons," in the December 2002 edition of *Privacy In Focus*). On appeal to the First Circuit, plaintiffs sought review only of the District Court's dismissal of the claim based on Title I of ECPA.

ECPA TITLE I

Title I of ECPA extended to data and electronic transmissions the protections that prior federal law had accorded to oral and wire communications. Title I, in relevant part, creates a private right of action against a party who "intentionally intercepts…any…electronic communication." "Intercept" is the "acquisition of the contents of any...electronic...communication through the use of any electronic…device." ECPA establishes a defence of prior consent to an interception, which either party to the communication may provide.

The issues before the Court of Appeals were whether Pharmatrak's service had constituted an impermissible "interception" and, if so, whether its pharmaceutical clients had "consented" to such interception. Taking the latter question first, the Court of Appeals held that the burden of proving consent, at least in a civil case, fell upon Pharmatrak. The Court ruled that the party claiming consent must prove either actual consent or, in its absence, show "convincingly" that implied consent was given.

PHARMATRAK'S ACTIONS CLASSED AS "INTERCEPTION"

Second, the Court of Appeals held that Pharmatrak's collection of personal data constituted an "interception" under ECPA. After discussing whether ECPA requires that an "interception" must occur contemporaneously with the transmission that is intercepted, or whether some delay is possible, the Court ruled that Pharmatrak was engaged in an interception under even the narrowest interception standard. Specifically, the Court concluded that Pharmatrak's obtaining the data in real-time was sufficient to constitute an "interception" under ECPA.

In so holding, the Court was unpersuaded by Pharmatrak's argument that two separate communications had occurred — one between the user and the pharmaceutical company site, and a second between the user and Pharmatrak. The Court found that contention immaterial, holding that ECPA does not necessarily require the acquisition to be the "same communication" as the intercepted "transmission". "Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement."

The Court remanded the case to the District Court for further action on whether the "intent" requirement of ECPA was satisfied. The issue had not been briefed, and the Court found the record unclear on whether Pharmatrak had acquired the personal information through technical glitches unknown to it. Citing legislative history, the Court noted that inadvertent interceptions do not provide a basis for civil or criminal liability under ECPA.

Consent to collections of personal data can be either express or implied, but both third-party providers and websites will want to address this topic directly in their contracting lest they become ensnarled in needless litigation.

NO CONSENT WAS GIVEN

On the facts, the Court ruled that consent was not present. Under the prevailing standard in the First Circuit, the Court ruled that the pharmaceutical companies' consent extended only to the communications that they had intended to allow. Said the Court: "Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of [the Pharmatrak service] on the fact that it would not collect such information."

The Court distinguished this case from *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) and *Chance v Avenue A, Inc.*, 165 F. Supp. 2d 1163 (W.D. Wash. 2001) on the grounds that, in those cases, the host websites had enlisted the services of DoubleClick and Avenue A for the purpose of creating user profiles.

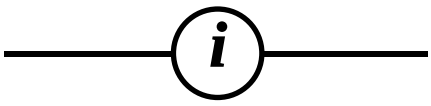
The Court also found that no consumer consent could be implied, because the pharmaceutical companies' websites "gave no indication that use meant consent to collection of personal information by a third party." The Court stated that "deficient notice will almost always defeat a claim of implied consent."

CASE IMPLICATIONS

The case is interesting for several reasons. First, the Court opted for a comparatively narrow definition of "consent" under ECPA. Under this approach, websites and in particular, third-party providers of monitoring services need to have clear understandings of what information is to be collected from or about web users. Consent to collections of personal data can be either express or implied, but both third-party providers and websites will want to address this topic directly in their contracting lest they become ensnarled in needless litigation.

Second, the Court held that third-party website monitoring could constitute an "interception" under ECPA. Accordingly, businesses engaged in profiling and tracking consumer data on other parties' websites must take steps to ensure that they do not run afoul of ECPA's restrictions, and may be at a competitive disadvantage relative to data-mining firms that do not monitor website activities.

Third, the Court did not address whether the use of "Web bugs" or "clear GIFs" is inherently illegal. Rather, the Court's analysis focused not on what the technology was, but rather on what it did. In that sense, the Court appears to have affirmed, at least in principle, the lower court's decision that web bugs are not, per se, nefarious or violations of ECPA.



AUTHOR: William B Baker is a partner in the Privacy, Internet & E-Commerce, Postal and Communications practices at Wiley Rein & Fielding in Washington, DC. He can be reached by telephone at: +1 202 719 7255 or E-mail: wbaker@wrf.com.

Benetton backs down over tracking technology

Plans to introduce hi-tech tracking devices into the retail sector have been met with stern opposition from consumer groups. **Eugene Oscapella** reports.

In apparent response to a boycott campaign launched by an American consumer interest group, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), the Benetton Group announced that it is not currently inserting tracking technology devices into its clothing. However, the global clothing retailer announced in the same April press release that it is now analysing RFID (Radio Frequency Identification) technology to evaluate its technical characteristics.

Benetton also announced that it reserved the right to "take the most appropriate decision to generate maximum value for its stakeholders and customers," suggesting that it has not discounted the use of such tracking devices in the future. The company produces and sells more than 100 million garments worldwide under its name.

CASPIAN's concern arose over a new consumer goods tracking system called Auto-ID, which couples radio frequency identification (RFID) technology with highly miniaturised computers. This permits products to be identified and tracked at any point along the supply chain. Each item would be uniquely identifiable through a numbering scheme called ePC ("electronic product code"). This would eventually replace the existing Universal Product Code (UPC). For example, tiny RFID devices (which Benetton refers to as "smart labels") could be implanted in clothing. An RFID reader could then identify the individual piece of clothing as it travelled from factory to transportation centre to retail shop.

Opponents of RFID fear uses of the technology can go far beyond simple inventory control. A purchase of clothing made with a credit card, for example, could link the purchaser and the item of clothing in a database. If the thirst for assembling masses of information in the name of national security and crime control continues (see, for example, "Total Information Awareness", *PL&B International*, Feb 2003, p.8) governments could use this tracking capability to monitor the movements of individuals through their clothing or other items they carry - without their knowledge or permission. Scanning devices placed at strategic locations - the entrance to a public gathering, for example - could identify any item of clothing or other product carrying an RFID chip.

> The European Central Bank is quietly working to embed RFID tags in the fibres of Euro bank notes by 2005...allowing police agencies to literally "follow the money"

Other databases may permit the items to be linked with a specific individual.

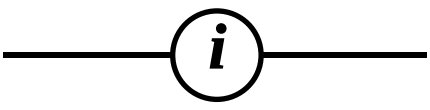
Katherine Albrecht, CASPIAN founder and director and a Harvard University doctoral candidate, spoke extensively about the potential secondary uses by government of such tracking devices at the April 2003 Computers, Freedom and Privacy Conference (CFP) in New York City and at the Privacy Activists Congress held the day after the CFP conference.

In a statement released in March urging the boycott of Benetton clothing, Albrecht explained the concerns about RFID technology: "Manufacturers of these chips are already promoting them as a way to track individuals and inventory their belongings. It would be easy for Benetton to link your name and credit card information to the serial number in your sweater, in essence 'registering' that sweater to you," she explained. "Then any time you go near an RFID reader device, the sweater could beam out your identity to anyone with access to the database - all without your knowledge or permission."

RFID technology can be highly miniaturised and will eventually become very inexpensive, according to Albrecht. RFID tags may cost less than one cent each by 2004, and can be as small as a grain of sand.

Albrecht also suggests that the European Central Bank is quietly working to embed RFID tags in the fibres of Euro bank notes by 2005. This would provide information about where the bank notes have been, allowing police agencies to literally "follow the money". "If and when RFID devices are embedded in banknotes," she wrote in one law journal article, "the anonymity that cash affords in consumer transactions will be eliminated."

What is the solution for consumers? Delegates at the CFP conference learned that the chips can be disabled by microwaving them - a new use for this staple kitchen product.



FURTHER INFORMATION: For details on the Benetton boycott, see: www.boycottbenetton.org/rfid_overview.html; www.boycottbenetton.org/press.html

Japan adopts a Personal Information Protection Law

Japan's new Privacy Law has the status of a basic law and signals a firm commitment by the government to drive forward a culture of privacy. **David E Case** and **Yuji Ogiwara** examine the new law and how it will affect the business community.

On May 23rd 2003, five bills were passed by the Japanese Diet relating to the use of personal information by government and private entities. This article focuses on the portions of the legislation applicable only to the use of personal information by private parties (the "Privacy Law").

On March 27th 2001, similar privacy legislation was introduced into the Diet for deliberation, but was finally left to expire in December 2002. The primary stumbling block was widespread criticism that the legislation would impair the freedom of journalists and academics. For a short while, it looked as if the legislation might not be passed by the end of the Diet session in mid-June, but a political compromise was reached and the legislation passed at the end of May.

The political compromise between the ruling parties led by the Liberal Democratic Party (LDP) and the Democratic Party of Japan (DPJ) that saved the new Privacy Law, should be of interest to privacy and data protection practitioners. First, the LDP and DPJ agreed to enact (or have promulgated by certain ministries) additional data protection laws and regulations targeting specific industries. Those industries selected are the medical, financial credit, and telecommunications sectors. The Privacy Law already applies to these industries, but it is presumed by people familiar with the new Privacy Law that the industry specific laws and regulations will provide additional detail as to how Personal Information (defined below) must be handled by companies in those industries. Second, the Privacy Law is totally open to revision in three years.

The most striking feature of the Privacy Law is that instead of being a detailed framework of laws and regulations regarding the collection and use of personal information, its provisions are very general.

THE PRIVACY LAW

The new Privacy Law establishes fundamental rules and a basic policy regarding the collection and use of personal information by private parties and public entities. A stated goal of the Privacy Law is to protect individual's rights and welfare. In its first article, the Privacy Law provides that the creation of an advanced information society in which personal information is used by public and private entities is a desired goal. The most striking feature of the Privacy Law is that instead of being a detailed framework of laws and regulations regarding the collection and use of personal information, its provisions are very general. Clearly, the Privacy Law is but a first step in the area of data protection law in Japan. Prior to the passage of the Privacy Law, the collection and use of personal information by the private sector was minimally regulated by some sectors' codes of practice.

FEATURES OF THE PRIVACY LAW

The Privacy Law is intended to set forth fundamental principles for collecting, using, handling and transferring personal information. Article 3 of the Privacy Law says:

> "In view of the fact that Personal Information should be treated with care based on the philosophy of respect for personality of an individual, personal information must be treated appropriately."

Due to concerns by the media and academia, a set of basic principles (contained in the previous version that failed to pass in December 2002) regarding the use of personal information was deleted from this version of the bill. The basic principles in the lapsed bill stated that personal information be:

1. used to the extent necessary to achieve a specific and appropriate purpose

2. acquired through a legal and appropriate manner

3. held in correct and current form

4. handled with safety and care; and

5. handled in a way that the underlying person shall be involved in the handling process.

Instead, these same principles are addressed elsewhere in the Privacy Law. Features of the Privacy Law follow.

PERSONAL INFORMATION

The definition of personal information is similar to that of other jurisdictions. "Personal information" (*Kojin Joho*) is information that relates to living individuals and which can be

used to identify specific individuals by name, date of birth, or other description - including that which can be easily compared with other information to identify specific individuals. The individual identified by personal information is called a principal or "individual" (*Hon-nin*). A collection of personal information structurally constituted so as to permit specific personal information to be easily retrieved electronically is called personal data (*Kojin Deta*). These definitions are set out in Article 2.

COVERED PERSONS AND ENTITIES

The Privacy Law is applicable to private parties and both national and local public entities, but under a separate set of rules. At this point, government entities are only obligated under the Privacy Law to establish basic policies concerning the protection of personal information in the future. As a result, the bulk of the Privacy Law's articles apply to private parties. A private party (either a person or business) that uses personal information in a business operation is called a "Business Handling Personal Information" (*Kojin Joho Toriatsukai Jigyo-sha*) or "business". The definition of a business is narrower than that of a "data controller" under the EU Data Protection Directive. The definition of a business expressly excludes:

1. organs of the national government

2. local public entities

3. certain independent administrative corporations; and

4. "persons designated by government ordinance as being little or no threat to the rights or welfare of individuals from the standpoint of the quantity of personal information handled and the method of use."

Any business that collects, handles or uses personal information, but holds fewer than 5,000 records, falls outside the law's coverage. One of the rationales behind this 5,000 record exemption was to permit small business owners, delivery truck operators and salespeople etc. that have programmed into their car navigation systems customer names, addresses and telephone information to continue to use such information without having to send to each individual a notice of what data has been collected and how it is used.

COLLECTION OF PERSONAL INFORMATION

Japan is an "opt-out" jurisdiction. It is up to individuals to limit or control the collection of their personal information. When collecting personal information, a business must describe to the extent possible (*dekiru kagiri*) its intended purpose of use for handling the personal information (the "purpose of use"). However, in Article 18, it states that a business need not inform the individual of its purpose of use if the business fears that its rights or fair profits will be harmed by such notification or by public announcement of the purpose of use.

The notice must either be given directly to the individual or be such that it places the individual in circumstances where they can easily learn the identity of the business, the purpose of use and the business' contact information. The latter method could come by way of a public announcement prior to the collection. If personal information is collected in connection with the execution of a contract or other document (such as an electronic form or record), the business must disclose its purpose of use to the individual in advance of such collection. Businesses are also obligated to draft and publicly announce a privacy policy.

A business may collect any type of personal information, but may not collect personal information beyond that which is required to achieve the disclosed purpose of use. Although there was some discussion in Japan regarding the introduction of an opt-in regime for the collection of sensitive information, the current version of the Privacy Law makes no distinction regarding the type of personal information being handled by businesses.

> Although, as a general rule, personal information may not be disclosed to third parties without the prior consent of the individual, the Privacy Law contains a series of generous exceptions that permits onward transfer in certain circumstances.

USE OF PERSONAL INFORMATION

Actual use by a business may not exceed a scope reasonably recognised as having an appropriate connection with the original purpose of use (Article 15). If a business changes its purpose of use, it must either directly notify the individual or publicly announce its revised purpose of use. Most Japanese licensed attorneys familiar with the Privacy Law believe that the phrase "except where that purpose of use has already been publicly announced" in Article 18(1) may be satisfied, depending on the situation, by publicly announcing such changes in a privacy policy on a website, by letter, or by announcement in a newspaper. Individuals may demand that a business cease using their personal data or stop providing personal data to a third party. But in either case, a business may refuse such a request if the cost or expense to do so is excessive.

If the business does not stop using the individual's personal information, substitute measures must be implemented to protect the rights and welfare of the individual. No guidance is given in the Privacy Law as to which rights of the individual must be protected. Generally though, the Privacy Law exempts a business' use or disclosure of personal information if pursuant to a law, ordinance or official order, or if necessary for the protection of human life, safety, or property, or if necessary to improve public hygiene or promote the health of children - provided that in these cases an exemption is used only when it is difficult to obtain the individual's consent (see, Article 16(3) of the Privacy Law).

CONTROLLING PERSONAL INFORMATION

A business must "diligently" maintain personal data in an accurate and up-to-date form to the extent necessary to achieve its intended purpose of use. At any time, individuals may request that their personal data be corrected or updated. The procedure by which individuals may request personal data to be corrected may be established by the business. As with the use of personal information, a business need not correct personal data if the cost or expense is excessive, provided the business implements some safeguard to protect the welfare of the individual. A business must also adopt measures to prevent unauthorised disclosure, loss or destruction of personal information within its control. Measures must include the appropriate supervision of employees who have access to personal information so as to achieve its security.

What is certain is that as various ministries draft industry-specific legislation and regulations, the privacy debate will heat up again in Japan.

ONWARD TRANSFER

Although, as a general rule, personal information may not be disclosed to third parties without the prior consent of the individual, the Privacy Law contains a series of generous exceptions that permits onward transfer in certain circumstances. There are three exceptions to what might normally be considered a disclosure or transfer of personal information to a third party.

First, a business may delegate some or all of the personal data processing or fulfillment function to a service provider or subcontractor. The service provider or subcontractor may be located inside or outside of Japan and no special conditions or forms of agreement are required by the Privacy Law in either situation. If a business delegates all or a portion of the handling of personal data, it must provide necessary and appropriate supervision of the service provider or subcontractor regarding security. Provided the business meets its obligation to implement appropriate supervision measures of the service provider, the service provider and not the business would be liable in the first instance for any misuse of personal information.

Second, disclosing personal information to a successor company as part of a merger is not a disclosure to a third party that requires the prior consent of an individual. The successor would be bound by the declared purpose of use, but could modify it as discussed above.

Third, sharing and joint use of personal information by businesses in the same field within similar purposes of use is also permitted, provided that the individual is given notice that personal information will be shared, or they have been placed in circumstances whereby such matters can be easily learned. For example, companies in the financial credit area, or travel agencies etc. may share information in providing their services. The purpose of use notice might be printed on the back of the ticket, for example. Another example is that a department store could send personal information to a shipping company in order for goods purchased by the individual to be delivered.

ENFORCEMENT

The obligations and penalties of the Privacy Law applicable to private parties will be enforced starting from a yet to be determined date set by government ordinance, but in any event no later two years from the Privacy Law's date of promulgation (*kofubi*). Depending on the type of business and the industry in which it operates, the ministry that typically has jurisdiction over the business activities of that business will also oversee compliance with the Privacy Law. No independent central agency has been appointed, although the Prime Minister may designate a specific minister or a committee of the National Public Safety Commission as the State Minister in Charge with respect to specific matters in handling of personal information by businesses.

PENALTIES

Finally, the Privacy Law has civil and criminal penalties ranging from admonishment orders, to fines of ¥100,000 to ¥300,000 ($850 to $2,600 or €720 to €2,150), and criminal sanctions. Penalties were absent from the previous version of the law and this was a source of much criticism.

CONCLUSION

Commentary written by Japanese scholars or attorneys regarding interpretation of the current version of the Privacy Law and its provisions will increase over the coming months. What is certain is that as various ministries draft industry-specific legislation and regulations, the privacy debate will heat up again in Japan. Details left out of the current Privacy Law will be filled in. Already, companies that extensively use or rely upon their customers' personal information to do business are approaching ministry officials with their concerns and suggested resolutions.

AUTHORS: David E Case is a senior associate at White & Case LLP Tokyo, practicing in the area of intellectual property licensing, litigation and acquisition. He currently serves as the co-chair of the Privacy Law Task Force of the American Chamber of Commerce in Japan. He can be contacted at Tel: +81 3 3259 0149 or by e-mail at: dcase@tokyo.whitecase.com.

Yuji Ogiwara is a senior associate at White & Case LLP Tokyo, practicing in the area of corporate, commercial, labour, intellectual property, litigation and transactions. He can be contacted at Tel: +81 3 3259 0156 or by e-mail at: yogiwara@tokyo.whitecase.com.

Ireland passes new privacy law

Carol Leland examines Ireland's new data protection law and looks at the impact it will have on private sector organisations.

Ireland has finally implemented the EU Data Protection Directive. Most provisions of the Data Protection (Amendment) Act 2003 ("the Act") will commence on July 1st. The Act amends the previous 1988 Act. The main changes bringing Ireland's data protection rules in line with the directive are:

• the Data Protection Law now covers paper files as well as computerised data

• consent will generally be required to process personal information (under the 1988 Act there was no specific requirement to obtain consent)

• the definition of sensitive data is extended to include trade union membership and ethnic origin, and can be processed only in certain circumstances

• automated decision making is generally prohibited

• individuals have more extensive rights over the information held on them

• universal registration replaces the current system of selective registration and;

• increased enforcement powers for the Irish Data Protection Commissioner.

JURISDICTION

The Act covers data controllers which are incorporated in Ireland, or which operate a branch or agency in Ireland, or which make use of equipment located in Ireland.

This raises the issue of the application of the Act to US (and other non-EU) businesses which operate back office operations (such as call centres) from Ireland. There are no formal guidelines on the issue, but the Data Protection Commissioner has indicated that the Act will apply to controllers who engage Irish-based processors. A non-EU controller who comes within the scope of the Act will be required to:

• nominate a representative in Ireland, but only if requested to do so by the Commissioner

• enter into a written contract with the Irish based processor; and

• ensure that adequate security measures are in place to protect the information.

Such a controller may sometimes need to amend customer documentation used in non-EU jurisdictions so as to meet Irish consent requirements, thus enabling the processing of the data in Ireland. Sometimes such consent may be implied or will emerge from existing documentation (or in the case of annual privacy notices issued by US financial services companies under US law).

APPLICATION OF THE LEGISLATION

The Act covers information about living individuals. It does not apply to the deceased or to information on corporate entities. In addition, the legislation does not cover:

• personal information processed for domestic purposes

• information which has been anonymised

• statistical data or data used for historical research; and

• information which the data controller is obliged by law to publish.

FAIR PROCESSING PRINCIPLES

The Act obliges data controllers to provide certain information to the data subject. The controller must at least inform the data subject of:

• the identity of the controller

• the purpose(s) for which the information is processed

• any other relevant information such as the recipients of the data, the existence of the right of access and the right to rectify data.

The legislation also gives effect to the other fair processing principles outlined in the directive (data must be accurate, up-to-date, and must be adequate, relevant and not excessive in relation to the purpose for which it was collected).

THE CONSENT REQUIREMENT

The data subject's consent is needed to allow processing, unless other specified requirements (mirroring those outlined in the directive) are met. Unlike the directive, the Act simply requires "consent" without specifying that the consent must be "unambiguous". However an Irish Court would interpret the Act in light of the directive and therefore the consent will need to be unambiguous.

SENSITIVE DATA

Sensitive data covers the following information: racial /ethnic origin; political opinions, religious or other beliefs; physical or mental health, sexual life; criminal convictions; trade union membership; and information relating to criminal prosecution.

Controllers must ensure that the fair processing principles are adhered to, but also that the processing falls within certain specific grounds set out in the legislation - for example, where there is explicit consent. The grounds in the Act include those in the directive along with the following additional grounds:

• where the processing is necessary to obtain information for statistical purposes and analysis (eg. a population census)

• where the processing is carried out by political parties or election candidates; and

• where the processing is carried out by revenue or tax authorities.

REGISTRATION

The new Act provides for universal registration, but allows the Minister for Justice Equality and Law Reform to exempt certain categories of data controllers from registration. There has been some resistance to universal registration, particularly by smaller and medium-sized companies. The registration provisions will not come into force until later this year, pending government consultation with businesses on an appropriate scheme for registration.

DIRECT MARKETING

A data subject must now be given an opportunity to "opt out" of receiving marketing information. The data subject also can require a data controller to stop using their information for direct marketing purposes at any time.

These provisions are supplemented by the European Communities (Data Protection and Privacy and Telecommunication) Regulations 2002 which are based on the European Data Privacy and Telecommunications Directive (97/66/EC). These regulations prohibit marketing by way of unsolicited telephone or fax calls unless the data subject has consented. An "opt-in" is required where the calls are automated.

INTERNATIONAL DATA TRANSFERS

The Act extends existing restrictions by prohibiting data transfers outside the European Economic Area (EEA), unless specified conditions are met. Transfers may take place if the data controller satisfies one of the following conditions:

• the destination country has been "white listed" by the European Commission or is a US safe harbour company

• the data subject has consented to the transfer of data

• the transfer is necessary to either comply with international law, is in connection with a legal claim, to protect the vital interests of the data subject, only comprises of information held on a public register, or is necessary for the performance of a contract; or

• the data exporter and the data importer enter into a contract; or

• the Commissioner approves the transfer.

For informed consent, the data subject should know which data is to be transferred, where it is being transferred and why. They may also need to be informed that the information may be transferred to a country which may not offer the same level of protection as the Irish law.

Consent can sometimes be implied. The Commissioner has indicated that consent is implied where employee data is transferred out of the EEA for routine HR purposes in the context of multinational operations.

Notification to the Data Protection Commissioner is not required where the data exporter and the data importer enter into a contract in the form approved by the European Commission ("model contracts"). However, where the parties deviate in any way from the model clauses, notification is required. Global or corporate policies will need the approval of the Commissioner.

POWERS OF THE COMMISSIONER

The Commissioner has increased enforcement and investigatory powers, including the power to conduct audits, and the power to devise and approve industry codes of practice.

The Commissioner has threatened to "carry out spot checks on public and private companies next year to ensure that they are in compliance with legal duties in the area." He has also claimed that his office "intended to visit banks and law firms to see if they had good data protection practices in place." Such activity would be a departure from historic practice as the Commissioner has not adopted a proactive enforcement policy to date, presumably due to limited resources and powers under the previous legislation.

PROHIBITION ON ENFORCED ACCESS REQUESTS BY EMPLOYERS

An employer may not require an employee to make an access request in order to provide personal information for the employer. This has particular significance where employers undertake background criminal checks or wish to verify qualifications of prospective employees. The employer may not make the employee ask the police or educational establishments for personal data. The employer may still make an application directly to the relevant body, but may require the individual's consent to do so. This provision will not commence until later this year.

PENALTIES

The Act creates various criminal offences which attract fines between €3,000 and €100,000:

• failure to register with the Data Protection Commissioner

• requiring a job applicant to make an access request

• failing to comply with a Prohibition Notice

• failure to comply with an Information Notice issued by the Commissioner

• unauthorised disclosure of data by a processor

• disclosure of data by a person who obtains the data unlawfully; and

• obstructing/impeding the Commissioner or any of his authorised officers.

The court may also order the forfeiture, destruction or erasure of any data. The court could foreseeably issue an Order that an entire database be erased in extreme circumstances. This could have obvious catastrophic consequences for any business.

Businesses could also be adversely affected by the publicity generated by a prosecution or an investigation by the Commissioner and this has been one of the Commissioner's main weapons under the former regime with certain cases attracting wide publicity.

AUTHOR: Carol Leland is an associate specialising in intellectual property and information technology law at A&L Goodbody. She can be contacted via e-mail at: cleland@algoodbody.ie

ADDITIONAL GUIDANCE: The Data Protection Commissioner has published a copy of the new law and compliance guidance on his website: www.dataprivacy.ie/7.htmwww.dataprivacy.ie/7.htm

Will Spain shift its hardline stance?

Spain's Data Protection Authority has earned itself the reputation of being one of the toughest privacy regulators in the world. But with a new Commissioner in charge, could the authority be steering towards a more business-friendly approach to compliance? By **Alan Pedersen**.

Notorious for imposing massive financial penalties and unafraid to take on global corporate giants, Spain's Data Protection Authority has adopted a rigid and uncompromising approach to privacy compliance. But, towards the end of April, its new Commissioner, Professor Dr Piñar Mañas, and key staff agreed to meet with the European Privacy Officers Network (EPON) to discuss its approach to corporate compliance.

ENFORCEMENT

Speaking at April's EPON meeting, Javier Fernández-Samaniego, attorney at law firm Linklaters, said the "approach to data protection in Spain, in my view, has been very focused on enforcement rather than dialogue with the private sector." In 2001, for example, the agency carried out 418 inspections, leading to 139 sanctions being imposed with fines totalling close to €10 million. High profile casualties include Microsoft, which was hit with a fine of around €50,000 in 2001 for failing to implement proper safeguards for transferring data to the US. And last year, global telecoms operator Telefonica was saddled with an €840,000 penalty after disclosing a customer's details to a subsidiary company without their consent.

Professor Mañas, however, defended the authority's actions, arguing that the Spanish courts have agreed with the majority of its decisions. He also indicated that the authority is unlikely to curb its tough stance on compliance, considering that widespread investigations into public sector organisations have yielded positive results and seen a drop in the number of complaints.

Nonetheless, he was keen to stress that the authority is not bent on singling out big businesses and hitting them with sanctions. "It is not an objective of this agency to be an authority establishing penalties," he said. "But, in the case of bad faith we will be very severe." He said that tough action is more likely to be reserved for repeat offenders and those who knowingly break the law.

On the positive side, he outlined his willingness to develop a more informal dialogue with the business community. "We are fully open to informal contacts and meetings," he said, adding that it is a standard procedure to meet with businesses, allowing the authority to point out flaws in companies' compliance procedures.

He also made supportive comments about multinational organisations, recognising that many are "prepared to make every possible effort to take preventative steps" and look at ways to solve ongoing problems. In fact, Professor Mañas said it is non-compliance in the public sector, rather than big businesses, that is the authority's primary concern. However, businesses should not be lulled into a false sense of security. Professor Mañas said results from 2002 indicated that there are still major compliance problems in the private sector with the majority of complaints relating to unsolicited marketing and credit reference data.

DATA TRANSFERS

The authority's approach to cross-border data transfers are set out in guidelines published in December 2000 (Instruction 1/2000 on International Data Transfers). "It is important for businesses to follow these guidelines," said Linklaters' Fernández-Samaniego, as the courts treat them as a kind of secondary legislation backing up the 1999 Data Protection Law.

The guidelines place some fairly onerous and arguably excessive conditions on businesses with lawyers pointing out that they effectively require prior approval from the Data Protection Authority for any international transfers – even if it is within the EU, or to countries that have been judged to provide an adequate level of privacy protection by the European Commission.

Mar Martínez Sánchez, head of the authority's General Data Protection Register, said it is a misconception that prior authorisation is required for all cross-border transfers. But, she added that organisations are required to register any transfers with the authority, which will then ask for proof that the organisation has a legal basis for the transfer. An organisation choosing to rely on consent for exporting HR data, said Sánchez, would have to supply documentation such as employee contracts to prove that consent has been properly obtained. If the information provided is insufficient or incorrect, the agency will reject the registration leaving the organisation in breach of the law should it proceed to export data outside Spain.

TRANSFER RULES CHALLENGED

The authority's regulatory regime was, however, dealt a blow in March 2002 when the Audiencia Nacional (Spain's superior court) annulled sections of the data transfer guidelines. It disagreed with Sánchez' analysis of the transfer procedures, ruling that the authority was unfairly imposing prior authorisation on transfers by requiring organisations to prove they have a legitimate right to export data.

Rather than viewing the ruling as a golden opportunity to change tack and pursue a more corporate-friendly course of action, Agustín Puente Escobar, head of the authority's legal department, said the authority decided to appeal against the Audiencia Nacional's decision. Confident of the outcome, he argued that there was no need to revise the guidelines, and stated that the authority will continue to enforce the guidelines until the appeal results come through - which may not be until 2004.

CONTRACTS

Furthermore, there is not much relief for companies choosing to use non-standard contracts (as opposed to the European Commission's standard contractual clauses) for cross-border transfers. Escobar said that although the authority can approve them, businesses are still required to comply with Spain's Data Protection Law and build in other guarantees such as third party rights and joint and several liability. It is not, therefore, an avenue that many companies appear to be pursuing. In fact, the authority only recently approved its first non-standard data controller-data controller contract for US-based John Deere Group. The contract, according to Sánchez, was approved because it closely matched the Commission's standard clauses and because the data subjects were given very specific information on the transfer process.

APPLYING THE NATIONAL LAW

Spain has adopted a very literal interpretation of Article 4 of the directive, which sketches out where and when the national law applies. But, Fernández-Samaniego said that such a rigid approach has caused problems for businesses. For example, a US-based company choosing to outsource its HR processing to Spain could be subject to the Spanish Data Protection Law (as well as some fairly stringent security regulations, see right hand box), even though the company and its employees are located outside the country.

Mar Martínez Sánchez said there are few companies importing data into Spain, but the authority would examine it on a case-by-case basis. The problems of applying the national law, she added, are more likely to affect US-based companies processing data for Spanish organisations, which again would be subject to Spanish law.

BALANCING INTERESTS

Another restrictive aspect of Spain's law is the fact that it has not implemented the "balance of interests" provision of the EU Data Protection Directive (Article 7(f)) - allowing organisations, under certain circumstances, to process personal data where they have a legitimate interest in doing do. It is an important provision for mergers and acquisitions, and companies going into administration, because outside parties need to examine employee data and getting consent is not really an option. The absence of a balance of interests, said Fernández-Samaniego, means that many companies in Spain are having to rely on consent to process HR data, which could leave them on potentially shaky ground from a legal perspective, especially since the EU Data Protection Working Party has expressed doubt over the validity of using consent in the employment context.

Agustín Puente Escobar cited two main problems over the balance of interest provisions. Firstly, there was the question of who actually makes the decision on whether the processing in question is legitimate. If businesses are allowed to interpret it on an *ad hoc* basis, individuals' privacy rights could be at risk, he said. Secondly, the structure of the Spanish constitution does not allow the government to draft a balance of interest provision into the Data Protection Law. However, Esobar did stress that balance can be achieved through other means, such as the creation of separate laws and regulations (for example, regulations on processing bad debtor/credit data). Businesses, however, have stressed that it would be unlikely that a separate law could be created for all eventualities where a balance of interest might normally apply.

FUTURE ACTION

Despite warm words from the Commissioner, expressing a desire to improve privacy by working with - rather than against - the business community, any signs of a softer line remain to be seen. The situation may become clearer later this year when Spain implements the EU E-communications Privacy Directive. Although the Spanish legislature is responsible for drafting the new law, it is likely that the authority will be tasked with drawing up guidelines on some of the more uncertain elements of the new law. However, its refusal to adopt a more lenient line on data transfers suggests it will continue to stick rigidly to the letter of the law – and beyond.

LEGAL TEXTS: For English translations of Spain's Data Protection Law, Security Regulations and its Instruction on data transfers, see: www.agenciaprotecciondatos.org/datd_inglish.htm

EPON: For details on the European Privacy Officers Network, contact Stewart Dresner, E-mail: stewart@privacylaws.com, or visit the PL&B website: www.privacylaws.com

Spain's Security Regulations

Spain has developed specific regulations on data security setting out three levels of security (basic, medium, and high) according to the type of data being processed.

BASIC SECURITY

Applies to every organisation that processes personal data. Requirements include establishing a security document which sets out the processing operations used by a particular organisation, the security procedures which are in place, procedures for reporting and managing incidents etc.

MEDIUM SECURITY

Applies mainly to data files containing sufficient information to obtain a picture of the data subjects' character/personality. This could theoretically apply to financial services organisations and credit reference agencies, and possibly marketing companies. In addition to the basic security requirements, organisations are required to appoint an officer in charge of security and perform a security audit at least every two years.

HIGH SECURITY

Applies to sensitive data and requires organisations to encrypt any data that is being transferred. Employers could find that staff health/medical data and payroll information could be subject to the high security requirements.

Commission reports uneven playing field for data protection

Kate Brimsted looks at the findings from the European Commission's investigation into the implementation of the EU Data Protection Directive.

On May 16th, the European Commission published its first report on the implementation of the Data Protection Directive (95/46/EC). The report is based on a review of EU member states' data protection laws, a wide consultation exercise which included an international conference, and an online survey that generated over 10,000 responses (*PL&B International,* Nov 2002, p.6).

The essential questions to be addressed by the report were whether the ways in which the member states have transposed the directive into national law achieve the ambitions of the directive. If not, what should be done to correct this? For example, should the directive itself be amended?

Several of the member states have been late in implementing the directive and France was singled out for criticism by Internal Market Commissioner, Frits Bolkestein, as it is still relying on data protection legislation dating back to 1978.

THE OVERALL PICTURE

The Commission expressed general satisfaction with the implementation of the directive and there are no current plans to amend it. However, the Commission recognised that, so far as ensuring a level playing field for operators in different member states and simplifying the regulatory environment, the differences between member states' laws and the directive are still too great. Amendments to national legislation are likely to be required in due course (this will be the subject of future reviews).

The Commission has proposed a work programme to address divergences in implementation and raise awareness.

SPECIFIC AREAS OF DIFFICULTY IDENTIFIED IN THE REPORT

The Commission's report highlighted the following key findings:

Sensitive and non-sensitive personal data - greater clarity on the "legitimate interests" condition was sought - this condition allows processing of non-sensitive personal data by data controllers without the subject's consent, provided that the legitimate interests, rights and freedoms of the individual are not overridden.

The Commission's view is that the absence of adequate safeguards means appropriate levels of protection for individuals are not currently being achieved.

> The Commission felt that [notification] problems were largely due to member states' failures to carry through the exemptions available in the directive.

Applicable data protection law – this topic came in for heavy criticism by respondents as, currently, organisations with a presence in (or which merely "use equipment" to process personal data in) more than one member state may have to comply with multiple national data protection laws. Submissions received argued for a "country of origin rule", allowing multinationals to operate via one set of rules throughout the EU. The Commission agreed that this area, and the term "use of equipment" in particular, needed clarification.

Legitimate processing conditions – these have been implemented unsatisfactorily in a number of jurisdictions, raising issues concerning appropriate safeguards and grounds for legitimate processing. In particular, the distinction between "unambiguous consent" (one of the conditions for lawful processing of non-sensitive personal data) and "explicit consent" (which is the level of consent required to process sensitive personal data) needs to be clarified to ensure uniformity across member states.

Provision of information to data subjects – in some jurisdictions, the law (wrongly) requires that certain "fair processing" information (for example, ensuring the data subject knows who the data controller is and the purposes for which his personal data are being processed) always has to be provided to the data subject, regardless of whether the individual already has that information or not. This causes significant difficulties for multinational companies doing business at pan-European level, especially via the Internet.

Notification requirements – many respondents argued that the notification process should be simplified on the grounds that it imposes a huge administrative burden on controllers without a commensurate improvement in protection for data subjects. The Commission felt that problems were largely due to member states' failures to carry through the exemptions available in the directive. For example, one such exemption currently under-employed by member states is the ability for controllers to appoint company privacy officers as an alternative to notification.

Exporting data outside the EEA – member states have diverged greatly on this business-critical issue. The directive mandates that (unless exempt) personal data may be transferred only to countries which ensure an adequate level of data protection. At present, some member states require almost no reference to be made to the national supervisory authority, whereas others require everything to be referred for authorisation, even where exemptions apply. The effect of this is likely to be that data exports will "switch to the 'least burdensome' point of export."

Subject access requests - despite calls for more flexible interpretation by those consulted, the Commission was not convinced (surprisingly, in the author's view) that this aspect of the directive was posing serious practical problems for controllers. The Commission relied on the 62 per cent of data controllers whose responses to its online questionnaire indicated that responding to subject access requests did not constitute an important effort for their organisation. However, as most of the respondents apparently either had no figures available or had received fewer than ten requests, it is possible that their responses reflect a lack of experience.

FUTURE PLANS

In response to concerns identified in the report, including on the levels of compliance, enforcement and awareness, the Commission intends to put in place a number of initiatives. A work programme for 2003-4 has been proposed which will include discussions between the Commission, member states and national data protection authorities. The Commission has also called for the Article 29 Data Protection Working Party to draw up proposals for a substantial simplification of notification requirements, more harmonised information requirements and for simplifying the international data transfer regime. Promoting PETs (Privacy Enhancing Technologies), self-regulation and raising awareness of data privacy rights were also highlighted as targets for improving data protection.

WHAT CHANGES CAN BUSINESSES EXPECT TO SEE?

Over the short-to-medium-term, the call for increased resources for national data protection authorities and initiatives to heighten the public's awareness of data protection rights can be expected to raise the compliance stakes for data controllers throughout the EU.

The sooner organisations put in place compliance programmes, the better the position they will find themselves in once the anticipated tougher enforcement regimes become a reality.

The outlook is not just weighted in favour of individuals however. At a detailed level there is recognition that the lack of consistency in data export restrictions, applicable law and notification obligations needs to be addressed.

So far as the notification regime is concerned, this can undoubtedly be simplified and one would expect the "data privacy officer" role to become more widely recognised in member states. This can be predicted to have a significantly beneficial impact on the corporate data privacy environment.

Regarding data exports, the Commission expects to see progress in four key areas: (1) more "approved country" findings; (2) a wider choice of recognised standard clauses for data export contracts; (3) the role of binding intra-corporate rules eg. group-wide data protection policies; and (4) more uniform interpretation of the exemptions. This will be heartily welcomed by businesses and can only promote smooth international data flows, with all the enhancements in information use and efficiencies these entail.

AUTHOR: Kate Brimsted is a senior assistant solicitor in the IP & Technology Department at Herbert Smith and a member of Herbert Smith's Data Privacy Working Group. She can be contacted via e-mail: kate.brimsted@herbertsmith.com

FURTHER INFORMATION: A copy of the Commission's report can be found at: http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm

EU survey reveals consumer discontent

Between June and September last year, the European Commission launched an online consumer consultation into the impact of the EU Data Protection Directive. The survey received 9,516 responses with the majority coming from Germany, France and the UK.

Analysis of the survey - recently published on the Commission's website - suggests consumers consider that governments are placing business concerns ahead of citizens' privacy rights. They believe that businesses are getting away with data protection breaches 'scot-free' and are especially concerned that health insurance companies are improperly collecting data from their doctors.

The report highlighted a general call for tougher regulatory sanctions with some respondents expressing the view that data protection authorities do not have enough powers.

Workers are happy to have e-mails read by their employers but only if they are business-related. One solution proposed by respondents was to provide workers with both a private and business e-mail address.

Some of the key figures from the survey include:

• 45 per cent consider their country to be providing a good-high level of protection

• 5 per cent think that there is not a good enough level of awareness among consumers

• 66 per cent are concerned that their personal data will be misused when using online services

• 56 per cent would like to see a positive opt-in rule for e-marketing

• 84 per cent are aware of 'invisible' data collection through the use of cookies and spyware technologies.

Hewlett-Packard faces the challenge of global training

Multinationals face the difficulty of providing consistent data protection training for staff in all locations. **Laura Linkomies** investigates how Hewlett-Packard delivers the same level of privacy training in all of its business units around the world.

Hewlett-Packard, a global provider of computer products and technologies, has to deal with the mammoth task of ensuring that its staff has sufficient data protection knowledge to comply with a multitude of global privacy laws. Due to the merger with Compaq Computer Corporation in 2002, the company now has 140,000 staff worldwide. For an organisation that operates in 160 countries, it is of paramount importance that staff training is consistent, and that there are no regional differences.

Daniel Pradelles, Hewlett-Packard's customer privacy manager for Europe, Middle East and Africa, explained to *PL&B International* that the company expects its entire staff to have a basic understanding of the most important privacy principles. Consequently, these principles are at the heart of the company's privacy training. The company offers three fundamental training programmes. "Standards of Business Conduct" is mandatory for all existing and new staff. "Respecting Privacy at Hewlett-Packard" is offered in two versions. The first version is mandatory for all staff who handle customer data, while the second has to be attended by all staff handling employee data. This is a minimum of two-to-three hours of training, which is followed by additional privacy training tailored to specific job functions and offered for staff that routinely deal with personal data.

THE BASIC RULES FOR ALL

The fundamental privacy principles that are explained during basic training are awareness, choice, access and accuracy, security and control. Daniel Pradelles emphasises the importance of every employee's familiarity with the fundamental privacy principles.

"These five privacy fundamentals should be known by heart by any employee who collects, handles or accesses personal data," he says, "with the ultimate objective to create a so-called 'privacy conscious culture' in the company.

By awareness, Hewlett-Packard means that it is essential to tell data subjects, whether they are employees or customers, what type of personal data is being collected, whether it is stored, and how it is shared with third parties. One of the best ways of getting this message through to customers is via the company's online privacy policy.

For an organisation that operates in 160 countries, it is of paramount importance that staff training is consistent, and that there are no regional differences.

"The purpose limitation principle also needs to be explained during the basic training," stresses Pradelles. "Staff need to understand that personal data may be collected only for legitimate purposes and in an amount which is not excessive according to the stated purpose."

After awareness, explains Pradelles, is the concept of choice. This refers to the customer's choice over how much personal data the company is provided with, the choice over whether or not a person agrees to share data with third parties, and so on.

"As a rule, Hewlett-Packard does not share customer data with third parties, but when we do, it is done only with the data subject's consent. The company also gives data subjects the choice to decide whether or not they want to be contacted by e-mail. Unsolicited mail, whether generated by Hewlett-Packard or not, is by far the most common customer complaint that the company receives."

"The company took the decision to require opt-in for e-mail in all our business units worldwide. In fact, this rule provides a higher level of protection than is required in some countries."

The principles of access and accuracy are also featured in Hewlett-Packard's basic training programme. The company makes sure that its customers and employees know that they have the right to access personal data held on them. The concept of subject access (by employees or customers) is also explained to Hewlett-Packard staff, as well as details on how to respond to these access requests.

The principle of security includes topics such as additional protection for sensitive data, and good business management processes to prevent unauthorised access and use of personal information. Staff also learn, in basic terms, how the company uses encryption to ensure a secure transfer of sensitive personal data.

"Lastly," says Pradelles, "we at Hewlett-Packard believe in feedback. We must provide our customers with a channel through which they can have their concerns heard and questions answered. We have set up a specific e-mail address, privacy@hp.com, which customers can use to contact us if they have any concerns over their privacy."

TRAINING ACCORDING TO SPECIFIC NEEDS

Hewlett-Packard collects a variety of personal data. Data is received from individuals as they order products and services, apply for credit, subscribe to marketing materials, register for products, and apply for, or accept, a job at Hewlett-Packard. Typically, the personal data collected includes name, address, phone number, e-mail address, user ID-passwords, and billing and transaction information. Personalised marketing, based on professional interests, demographics, and experiences with Hewlett-Packard's products or services is only carried out for those who have proactively agreed to provide that information.

Understandably, a Hewlett-Packard employee who deals with financial or other sensitive data needs to be more aware of data protection rules than someone who seldom comes across personal data as part of their daily work routine. The company organises specific data protection training for employees working in marketing, call centres and in web design. The company also ensures that any third party contractors are trained according to its standards.

A MIX OF DIFFERENT METHODS

"Hewlett-Packard uses a variety of different training methods depending on the audience," explains Pradelles. "While computer-based training is widely used, training seminars and workshops are used for more specific training. We organise a bi-monthly "Privacy Expert Seminar", which is intended to 'feel the privacy trends', and share experience and views. This one-day seminar typically features external speakers from the worldwide privacy community, major businesses and consulting companies. The basic training is also supported by an intranet web and an internal e-mail system, whereby employees can address any concerns they may have."

The company has three main websites with links between them. In addition to the Corporate Privacy Office's website, the company has websites for the Customer Privacy Team and the Employee Privacy Team. These websites include reference materials, guidelines, policies, slide sets, and tools to design new programmes and applications, or assess existing ones. Staff can also always contact the privacy teams directly by phone.

TRAINING MAINLY IN-HOUSE

Most of the training is delivered by the company's own privacy team, which is spread around the world. Pradelles, customer privacy manager for Europe, Middle East and Africa, is based in France, and has a counterpart based in Germany, who is responsible for employee privacy.

In the US, there are three privacy teams that concentrate on different areas (the chief privacy officer is based in California, the worldwide customer privacy officer is based in Texas and the worldwide employee privacy officer in Colorado). Australia has its own customer/employee privacy officer.

> "In a large, complex and diverse company dealing with so many different countries, legal systems, cultures and sensitivities, there is a real challenge to maintain consistency, and ensure flexibility and timely adaptation to business constraints."
>
> **Daniel Pradelles, Hewlett-Packard**

"As you can see, we are a truly international team, remote from each other, but very well and tightly coordinated," says Pradelles. "The main form of communication between the teams is e-mail and weekly teleconferences."

"The reason why we have divided privacy implementation between customer and employee privacy is that even when the concepts and laws are the same, the actual implementation, scope, systems architecture, audience, data subject groups and complexity are quite different," he continues.

FOLLOW-UP FORMS PART OF TRAINING

Asked whether the company evaluates how well the training has been received, Pradelles explains that at the end of a training course, participants fill in an evaluation form which is used for feedback. The company does not currently test staff on their data protection knowledge, but is in the process of developing a survey and self-auditing practices which will address this point.

As maintaining data protection awareness is just as important as formal training, the company has set up an extensive network of 'Privacy Champions' and 'Advocates'.

"In a large, complex and diverse company dealing with so many different countries, legal systems, cultures and sensitivities, there is a real challenge to maintain consistency, and ensure flexibility and timely adaptation to business constraints," says Pradelles. "To reach these goals Hewlett-Packard has set up flexible and efficient links between the business organisations in the field, and us, the privacy team. The "Privacy Champions" are managers who work at the worldwide and regional level. They support the implementation of our privacy programmes. The so-called "Advocates", who are privacy knowledgeable people working in the main business units - marketing, call centres, HR, finance, e-business - spread the word about privacy at the operational level. These are the people who make it real for the rest of the staff."

"In addition to all this, websites, our monthly internal "privacy newsletter" with privacy news, tips and advice about best practice, are also a powerful way to maintain awareness," sums up Pradelles.

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

STAFF TRAINING: For information about *Privacy Laws & Business* data protection staff training services, contact Sandra Kelman, Tel: +44 (0)208 423 1300, E-mail: sandra@privacylaws.com

Conference report: Privacy Laws and Effective Workplace Investigations

The privacy implications of workplace investigations was the theme of a Vancouver conference held by Insight Information, April 23-24th. The conference examined a broad range of issues, from means to make organisations privacy compliant, to privacy rights and sexual harassment in the workplace. Over the next four pages, **Eugene Oscapella** highlights some of the key issues addressed at the conference.

Building a culture of respect for privacy among employees

How can organisations encourage employees to share their vision of a privacy-compliant workplace?

Former British Columbia Information and Privacy Commissioner Dr David Flaherty, now a privacy consultant, stated his concern about the extent of unauthorised access to personal information occurring in public institutions by individuals who do not have a "right to know". This situation was worsening because of the increasing number of automated data storage systems held by groups such as the police, and in institutions such as hospitals.

The inspiration for such collection, argued Flaherty, may simply be the power that flows from holding information. He cited as one example a Canadian police officer who was opposed to abortion and who had used his police computer to obtain information about individuals attending an abortion clinic from the licence plates on their cars parked at the clinic.

In an environment of unauthorised access, claimed Flaherty, it is very difficult to create a culture of respect for privacy. Still, there are ways to succeed.

Introducing a culture of privacy is like introducing any other form of "cultural" change to an organisation. The same kinds of skills that are brought to bear on any other management issue must be used to introduce a culture of privacy. It requires consciousness-raising "from the top down and bottom up". Everyone in management must be made to understand privacy issues. Human resources professionals, he suggested, generally have a very good understanding of privacy issues; many fair information practices are likely already ingrained with them. The challenge is to expand this knowledge throughout the organisation.

> an organisation's privacy culture requires maintenance and continuous improvements through audits and onsite visits

Flaherty identified a series of prerequisites for creating a culture of privacy. First, privacy policies must be known and understood. Procedures to complement those policies must also be established. Furthermore, the more "privacy intensive" the nature of an organisation's work (a hospital vs a hardware store, for example), the more seriously it must take privacy.

Frequently Asked Questions (FAQs), he stated, are an effective way to help employees and customers understand the implications of privacy. For example, customers need to be told what information is collected about them and what is done with it. Often, these FAQs can be modelled on those from other sites.

Creating an awareness of the importance of privacy cannot be a one-time activity. Privacy team members must "have their noses to the ground," said Flaherty. "They have to mix with the troops." Organisational intranets can also be used to maintain awareness and inform employees of developments and issues.

Training, he added, is the key to effective implementation of a privacy culture. It may be best to have human resources training experts identify how to communicate information most effectively, since the type and amount of training required will vary among employees. Training can be accomplished through online programmes, intranet communications and by adding privacy modules to existing organisational training programmes. Once training begins, it will also be necessary to identify the individual or individuals responsible for responding

to questions about privacy issues. The questions fielded by such individuals will help identify the issues that need to be addressed in the organisation's privacy FAQs.

Establishing accountability is also an essential building block for a privacy culture. Organisational management teams were initially sceptical of the concept of the Chief Privacy Officer (CPO). Now, however, more are convinced of the need. The CPO should report directly to senior management - preferably the Chief Information Officer (CIO) or CEO.

Flaherty also recommended building a privacy "team" to address ongoing privacy issues. Representatives from legal affairs, human resources, communications, IT, marketing, the CIO, and senior management should meet periodically to try and solve problems internally. In addition, a crisis management approach must be put in place in advance of any possible privacy crisis. "How will the organisation respond when a reporter calls to ask what happened to records that fell off the back of a truck?" asked Flaherty.

The CPO can be particularly useful in establishing an internal process to resolve privacy issues, thereby avoiding customers or employees appealing directly to the "privacy police" - privacy or data protection authorities. However, the CPO cannot be expected to resolve all privacy issues. It may be necessary to devolve responsibility to others for certain decisions relating to privacy. For example, the level of privacy risks that a company should tolerate may be a decision to be made by the CEO, not the CPO.

Even once established, an organisation's privacy culture requires maintenance and continuous improvements through audits and onsite visits, says Flaherty. The organisation must ensure that privacy rules and procedures work in practice. Audit trails are an obvious tool. CPOs could even consider proactive ongoing auditing. Furthermore, technology can increasingly be used to build in "privacy by design".

Privacy officers must keep their eyes open. What they see in onsite visits - for example, a fax machine in a public area, with sensitive documents thrown into a nearby trash bin - may help them act in time to avoid a privacy crisis.

Using computer forensics to combat e-theft

According to consultancy firm KPMG, hi-tech information thefts carried out by employees are requiring businesses to adopt an increasingly sophisticated approach to investigations.

Owen Key and Brent Homberger, both of KPMG Forensic Technology Services, explained how dishonest employees sometimes use highly sophisticated programs to steal corporate information. Hi-tech thefts from corporations, they noted, are mostly internal, involving current or past employees, contractors, cleaning staff, or the relatives of any of these. Their presentation described the role of computer forensics in obtaining and preserving evidence of improper activities.

Computer forensics involves preserving electronic evidence in its original state to enable others to restore the information and obtain the same results, should this be required. In short, computer forensics take a snapshot (not a copy) at a given point of time of a piece of information that may be stored electronically. Simply copying files from an employee's computer is not a good forensic technique, since it changes the times associated with the documents. Computer forensics involves backing up information in a form that does not change the media and the associated times. As with other forms of evidence in legal proceedings, forensic investigators are seeking to prove the "chain of evidence" and that the evidence is authentic.

Key and Homberger explained that hitting the "delete" button does not mean that the information disappears from the computer's hard drive. This action merely tells the computer that these files can be overwritten, but the files may nonetheless remain partially or wholly intact on the computer for years. Nor does formatting a hard drive mean that information is gone from the computer. It simply means that the index has been changed. Forensic investigators are able to rebuild the index.

Key and Homberger argued that corporate IT experts do not have the legal background to understand the needs of forensic investigators. In other words, forensic investigation is a police issue, not an IT issue.

They used an example of a disgruntled employee using technology to steal a company's intellectual property. Forensic investigators may perform several tasks to catch such an employee: recovering damaged or deleted files; identifying and restoring files; identifying user-created files; searching the "slack" space areas of a hard drive, circumventing password protection and encryption; examining e-mails and temporary Internet files; identifying "cookies"; monitoring the computer network; and examining security log records. These actions, coupled with witness statements and timesheets, enable investigators to build a profile of the employee and follow the employee's actions.

Key and Homberger also described the potential of camera technology for catching dishonest employees. Older technology used photocells, videotape and "lots of wiring," they said. New technology is much simpler to employ and may specify what triggers a camera to activate - for example, someone tapping on a computer keyboard. This can then be monitored from practically anywhere. The technology can also be structured so that both the employee and the screen can be monitored at the same time.

However, they noted, the intrusive nature of these forensic investigations requires attention to the privacy expectations of employees - particularly when the investigation captures the activities of, or information about, third parties who have nothing to do with the conduct under investigation.

Investigating sexual harassment and romance in the workplace

Investigations into claims of workplace sexual harassment throw up some problematic dilemmas for employers when deciding the information which they can and cannot disclose.

"All workplaces are different. Every complaint is different. As a result, there is no set format for investigating sexual harassment complaints," cautioned Sue Paish, QC, a Vancouver-based lawyer whose practice centres on employment and human rights law.

Employers in Canada have a legal duty to deal with complaints of harassment that violate human rights codes. Despite the longstanding existence of sexual harassment policies in many Canadian workplaces, Paish stated, many employers may not be comfortable with the investigation or other processes involved in the policy.

Yet an effective investigation process promises several benefits, she said. It increases the likelihood of preventing other incidents, protects the company and employees from litigation and brings overall credibility to the harassment policy. Besides, it is the "right" thing to do.

Paish's presentation focussed on several aspects of investigating such complaints. At the heart of any good investigation, she noted, lies a good investigator acting solely as a fact-finder. A central need of the investigation process is the safeguarding of confidentiality. However, investigators may not be able to control what is done with personal information once it leaves their hands. Investigators should, therefore, get consent for what may be done with the information, to comply with any relevant legislation and legal obligations. Ideally, complainants should sign a form saying that they understand there may be a disclosure of information.

The complainant generally has no right to detailed information about measures taken to address the harassment. The complainant might be told only that measures have been taken to address the situation.

KEEPING CONFIDENTIALITY

No matter how well-designed a harassment process is, employees will not use it unless information is kept confidential, said Paish. Not only must the confidentiality of the complainant be protected, but also that of the respondent. Otherwise, the respondent is effectively being pre-judged. In addition, all participants in the investigation process should be assured that the information they provide will be kept confidential. However, there can be no anonymity in the complaints process, since the respondent has a right to know the identity of the complainant and a detailed description of the complaint.

By having a lawyer act as an external investigator, the report and information may be protected under the concept of legal privilege.

EXTERNAL INVESTIGATIONS

By having a lawyer act as an external investigator, Paish stated, the report and information may be protected under the concept of legal privilege. This may be particularly useful where data protection legislation might otherwise give parties rights of access to documents relating to the investigation.

Paish also advised employers to have a plan for handling evidence. The evidence should be kept after the investigation. It must be kept securely. It should be segregated from normal personnel files.

Employers may also need to be concerned about consensual office romances because of potential breaches of trust, conflicts of interest, or favouritism. However, unlike the United States, blanket anti-fraternisation rules are generally not upheld in Canada. Paish suggested that employers can instead rely on conflict of interest rules and disclosure policies to avoid potential problems, especially where there is a supervisor-supervised relationship.

Paish noted that under data protection legislation, such as the British Columbia Freedom of Information and Protection of Privacy Act, public sector employees who have been the subject of harassment complaints may apply to have the information collected during the investigation disclosed to them. However, she noted, a number of exceptions in the law often work to prevent harassment investigations from being disclosed. For example, information cannot be disclosed if doing so would harm the privacy of a third person.

Dealing with drug and alcohol incidents

Employers wanting to stamp out drug and alcohol abuse in the workplace will need to take into account a number of privacy safeguards if they wish to stay the right side of the law.

Victor Leginsky, a Vancouver-based management industrial relations lawyer, examined the motivation for employment drug testing and the privacy issues that flowed from testing. Drug testing, he argued, is becoming more common, but it must be considered against a backdrop of privacy and human rights laws and cases.

Employers, he said, have several motivations for an interest in workplace drug testing. They want maximum employee productivity and a safe working environment for employees and the public. Employers are entitled to manage their work sites and may prohibit alcohol and drugs and require employees to be unimpaired while at work. However, employees have a right to be free from employer intrusions into their off-duty lives.

Leginsky cautioned that it was important to "do the math". Are employees coming to work impaired or missing work due to alcohol or drugs? Employers must be able to defend a drug testing policy by demonstrating a problem caused by alcohol or drugs. Drug testing policies based simply on morality (he cited the US "war on drugs") will fail. Labour arbitrators look to see if the employer is being reasonable in all contexts. This also applies to decisions to introduce alcohol and drug testing.

He also warned of the obstacles confronting organisations that consider drug testing. Workers are already worried about the mass of data kept about them by employers. The results of drug testing will add to this, possibly revealing information not related to the purpose of the drug tests - the use of "recreational" drugs outside working hours, diabetes or pregnancy, for example. Being subjected to a drug test is possibly discriminatory, and also degrading, since employees must produce a urine sample while being watched to ensure validity of the sample. The tests themselves may also be unreliable.

Furthermore, alcohol and drug dependencies are considered disabilities under human rights laws in many jurisdictions. Employers have a duty to "accommodate" employees with disabilities, and dismissal based on alcohol or drug dependency may be prohibited under those laws.

Privacy legislation may add additional elements to the issue. Consent from those being tested may need to be more specific for the disclosure of health-related information (drug testing provides "health information") than for other types of personal information. Employers must build in specific consent for the collection of urine samples, and identify the disclosures of test results. Ideally, such consent should be obtained at the time of hiring a particular employee. Any drug testing policy must also explain its purpose, demonstrate the need for testing, the consequences of testing positive or refusing to be tested.

Leginsky cautioned that employers in Canada probably cannot require employees to be drug and alcohol-free 24 hours a day. He also reminded the audience that drug tests, unlike alcohol tests, cannot identify whether the employee was impaired at the time of the test. He suggested that it would be very difficult to justify pre-hiring or random testing as a "bona fide occupational requirement" under human rights legislation. However, random testing may be easier to justify in safety sensitive positions. "For cause" testing (for example, when an employee is seen drinking on the job) and post-accident/incident testing are more easily justified, as is testing on the return of an employee from an alcohol or drug treatment programme.

French law on privacy in the workplace

The debate concerning employers' versus employees' rights in France is not a new one. But, says **Nancy E Muenchinger**, the development of new technologies in the workplace has meant that the entire subject has once again come to the forefront of the judicial landscape and is having to be seriously rethought.

"The dividing line [between the tie of subordination and private life] can no longer be drawn at the door of the workplace and the end of the work day. Everything has become more complex and more blurred" *(Rapport pour le Ministre du Travail, de l'Emploi et de la Formation Professionnelle, December 1991, Documentation Française, Professor Gérard Lyon-Caen).*

In 1991, when these words were written, they set the groundwork for the law of December 31st, 1992 on Employment, Part-Time Work and Unemployment. This law was devised to implement a "Law on Information Technology and Human Rights" in the workplace to parallel the existing data protection law of January 6th, 1978, known as the "Loi Informatique et Libertés".

The principal tenets of the employment law of December 31st, 1992 were:

1. The principle of "finalité" (purpose) and of proportionality

> "No one can place restrictions on individual and collective rights which are not justified by the nature of the task to be performed and are not proportional to end sought" - **Article 120-2 of the Labour Code**.

This provision has been interpreted so as to allow employers to place restrictions on employee privacy which are justified by the circumstances. For example, in one case it was held that an employer, who was concerned by bomb alerts, legitimately allowed the opening of handbags in front of security agents. The action was justified by exceptional circumstances and was proportional to the objective, in that there was no full-scale search of the handbags.

2. The principle of transparency

The employers' obligation of transparency takes several forms.

a. Consultation of the Works Council

> "The Works Council is [to be] informed and consulted prior to any important plan for introduction of new technologies, when these are susceptible of having consequences on employment, qualifications, remuneration, training, or the conditions of work of personnel" - **Article L-432-2.**

The introduction of "new technologies" has been held to include the implementation of a new computer information system in a bank, when the system was significantly different from the previous one and it required special training. Even the replacement of a third generation computer by a higher performance model has qualified as "new technologies".

Moreover, the Works Council "is [to be] informed prior to any implementation in the enterprise of methods and techniques permitting the control of employees" - **Article L-432-2-1 section 3.**

Such "methods and techniques" would not only include electronic identification and entry systems and video cameras, but also special software used to establish Internet usage, websites visited, connection times, etc.

b. Prior information of salaried workers

> "No information concerning a salaried employee or a candidate for employment may be collected by any means which has not previously been brought to the attention of the employee or the candidate" - **Article L121-8 of the Labour Code.**

This requirement is significant in that it places the burden of informing an employee about monitoring squarely on the employer, rather than on an employee to obtain the means to inform himself. Thus the presence of a monitoring device such as video surveillance equipment in plain view does not do away with the employer's obligation to inform his staff that they are being monitored.

Another aspect of the employer's obligation of transparency toward employees relates to recruitment techniques:

> "A job candidate must be explicitly informed, prior to implementation, of methods and techniques aiding recruitment which are used in regard to him" **- Art L121-7 of French Labour Code.**

In one case, which was judged prior to the effective date of Article L121-7, a company required a handwriting analysis of a job application letter, and the candidate had had his wife write his letter. The court held that the company bore the burden of proving that it would not have hired the candidate in the absence of the tactics which he had employed to obtain the job.

FRENCH DATA PROTECTION LAW: THE LAW OF JANUARY 6TH, 1978

A law created to prevent data collection on individuals interfering with human rights was enacted early on by French legislators. The Law on Information Technology and Human Rights ("Loi Informatique et Libertés"), referred to above and passed on January 6th, 1978, was a precursor to similar laws of its kind in Europe. This law formalised the principle that:

> "information technology must be at the service of the citizen...It must not be detrimental to human identity, human rights, private life, individual or collective liberties" **- Article 1.**

The law created a data protection authority called the Commission Nationale de l'Informatique et des Libertés (CNIL) which acts as a kind of central clearinghouse for all questions concerning data protection. The principal mechanism of the law is the requirement of a declaration: any data processing treatment of "nominative information" (ie. information which identifies or is susceptible of identifying a named individual) must, prior to its implementation, be the subject of a declaration to the CNIL. Thus, any employers wanting to compile databases on their French employees must first proceed to make a declaration to the CNIL.

The latest version of the revised draft law implementing the EU Data Protection Directive (95/46/EC) (after adoption on first reading by the Senate) provides that declarations and requests for authorisation must include:

1. the identity and address of the data controller (employer) or its representative, if it is not established on national territory

2. the purpose(s) of the data processing and the general description of its functions

3. the interconnections with other data processing

4. the personal data processed; its origin and the categories of individuals involved

5. the duration of conservation of the information processed information

6. the services responsible for implementing the processed

7. the parties intended to receive transmission of the data

8. the function of the person or the department providing access to the relevant individuals

9. the security measures to be employed in relation to the data; and

10. the transfers of personal data intended for transmission to non-EU member states.

The same draft requires that all persons from whom data is collected, and thus by extension, employees, be informed of certain aspects of the data collection, namely:

1. the identity of the controller (employer) or of its representative

2. the intended purpose(s) of the data collection

3. the obligatory or optional nature of the reply

4. the consequences of a failure to reply

5. the parties destined to receive the data

6. the data subject/employee's right to access, oppose, or correct data collected; and

7. if applicable, of transfers of data to non-EU member states.

Thus, in addition to its obligation to notify any actions involving technological monitoring in the workplace, the employer must notify employees about the compilation of databases of information concerning them and the uses to which it will be put, including any transfers to a parent company.

It should be noted that the basic obligation to notify data subjects/employees was not instituted by the EU Data Protection Directive. The provision, which already exists under the 1978 law, has merely been updated under the terms of the transposition draft.

Concerning the privacy of its employees, the employer is therefore constrained to deal with a fairly onerous system of principles and rights of employees which act as a type of direct counterbalance to the tie of subordination characterising the employer-employee relationship in France.

Beyond the above specifics, it is important to note that the entire regime on the protection of personal data in France is undergoing profound changes at the moment. Pending the adoption of the draft law, there are still many questions being posed by employers and others to which there are not always clear answers. But at least one element remains stable, and that is the key space which the CNIL will occupy in this sector in the future. In the absence of clear-cut procedures, some companies are making a regular practice of consulting the CNIL for an opinion, rather than waiting for the legislative to be finalised. This is one indication of the increase in power and stature of the CNIL in the last several years, and is a trend which is not likely to be reversed.

SECRECY OF CORRESPONDENCE: THE LAW OF JULY 10TH, 1991 RELATIVE TO SECRECY OF CORRESPONDENCE

Before the introduction of e-mail on the scale attributable to the growth of Internet, there was already existing legislation protecting the secrecy of correspondence that was susceptible of applying to e-mail. Hence, an employer who, in bad faith, engages in "opening, deleting, delaying or diverting correspondence addressed to a third party, whether or not it has arrived at its destination" may be punished by a year in prison or a fine of €45,000 **- Article 226-15 of France's Criminal Code.**

Furthermore, the "fact of [an employer's] intercepting, misappropriating, using or disclosing the correspondence emitted, transmitted or received by a telecommunications network or proceeding to install devices conceived to affect such interceptions" would be punished by the same penalties **- Article 226-15(2).**

The legislation clearly targets all types of networks and telecommunications. The definition of "correspondence" provided in the Postal and Telecommunications Code includes "any transmission, emission, or reception of signals, writings, images, sounds, or information of any nature by optical wire, radio electricity, or other electromagnetic system" **- Article L.32 of Postal and Telecommunications Code**. Thus, employee use of Internet messaging, Minitel, faxes and Intranet, in addition to simple telephone calls, all fall clearly within its scope.

COMPUTER FRAUD: THE LAW OF JANUARY 5TH, 1988 OR "LOI GODFRAIN"

In addition to the types of prohibitions listed above, based on telecommunications law, another regime applies to, and protects, information systems from pirating and computer fraud. This regime is the so-called "Loi Godfrain", which went into effect on January 5th, 1988.

The "Loi Godfrain" places criminal sanctions on (1) the fact of acceding or maintaining oneself fraudulently in all or part of an automated data processing system (one year imprisonment and €15,000 in fines); (2) the fact of impeding or falsifying the functioning of an automated data processing system (three years imprisonment and €45,000 in fines); (3) the fact of introducing data fraudulently into an automated data processing system or deleting or modifying the data which it contains (two years imprisonment and €30,000 in fines) **- Article 323-1 and 323-2 of French Penal Code.**

These provisions, although theoretically applicable to employers, might be more difficult to maintain and to prove against an employer when the data processing system is clearly his own creation, it is under the virtually complete control of a systems administrator hired by the employer, and this administrator is responsible for the architecture of the system, as well as its day-to-day operations.

WORKPLACE PRIVACY CASE LAW: E-MAIL AND INTERNET USE

After some initial hesitation, French judges have come down firmly on the side of employee rights in relation to e-mail monitoring and Internet use. Some of the cases have dealt with personal use of Internet and the potential abuse that can occur, while others have dealt more directly with the concept of violation of correspondence.

In one of the former cases involving IBM, the Employment Court of Nanterre handed down a judgment on July 16th 1999, condemning the employer for wrongful dismissal. IBM had fired one of its employees for gross misconduct in connecting to and downloading onto his hard disk, various files from websites "covering a full range of pornographic practices". However, the court found the employer had not borne the burden of proof of its allegations, since the hard disk had not been under seal following its seizure, and the photographs produced bore dates that were subsequent to the facts, or no date at all. Moreover, an internal document that IBM produced as evidence that it had provided warnings to employees against sexual surfing, did not refer explicitly to this practice. As a result, the company lost the case.

In a second case confirming the trend, the Court of Appeals of Montpellier found imperative the obligation to inform employees as to telephone wiretapping or Internet e-mail monitoring prior to the implementation of employer controls. The facts in that case were that an employee with 16 years of service had used his workstation in a fraudulent manner by sending many e-mail messages during and outside working hours. The terms of the dismissal letter mentioned evidence that had been obtained from a "huissier", or sheriff, in the absence of the employee, and without his authorisation. The only document which the employer had been able to show by way of proof of notice, was a letter sent to the employee at the time of the installation of his computer system - the letter did not mention monitoring at all.

After some initial hesitation, French judges have come down firmly on the side of employee rights in relation to e-mail monitoring and Internet use.

The Court held that the employer had failed to establish gross misconduct justifying the dismissal, and awarded the employee damages equal to six months' salary.

Among the cases dealing with the violation of private correspondence by an employer, two are worthy of note. In the first case, the Tribunal de Grande Instance de Paris (TGI) formally accepted the principle that an electronic mail message constitutes private correspondence, by its decision of November 2nd, 2000.

The case can by summarised briefly as follows: An IT student from Kuwait filed a criminal complaint with the judge (of criminal instruction) alleging (1) theft; (2) opening of private correspondence; and (3) discrimination, ostensibly based on a romantic disagreement.

Three civil servants with a public service role at the "Ecole Supérieure de Physique et de Chimie Industrielle" acknowledged their actions, but maintained that they had acted to preserve the security of the school's network. The court disagreed and said that the motive of "good faith" was immaterial in a case of a criminal act committed by an official of a public service.

The opening of the e-mails on the school network was held to be a violation of the principle of privacy of correspondence under Article 432-9 of the Penal Code. This article provides that a public authority may not abuse its power by ordering, committing, or facilitating the interception or redirection of correspondence sent by means of

telecommunications networks, nor may it use or disclose their contents.

The second case was a landmark decision of the French Supreme Court involving the dismissal in 1995 of an employee of Nikon, for gross misconduct owing to the sending of numerous personal e-mails during working hours. To obtain proof of the employee's actions, the employer had opened and copied onto a diskette a file marked "personal" in the employee's absence. The French Supreme Court found that:

> "an employer cannot read the personal e-mail messages sent by the employee and received by him on a computer placed at his disposition for his work, without infringing his fundamental freedoms, even in the event that the employer has expressly prohibited the use of the computer for non-work related purposes."

The French High Court by this case thus placed important limits on the employer's power to control and monitor its employees during their work hours. In effect, it has carved out a right to protection of private life and a right to secrecy of correspondence which must be respected, even in the workplace and during work time.

CNIL REPORTS

Amid the doubts raised by the recent and sometimes conflicting court decisions, the CNIL has issued two reports relating to e-mail monitoring. The reports contain the main points of the CNIL's recommendations on employees' privacy in the workplace, and the employer's monitoring rights for security reasons. The reports include proposals such as *a posteriori* monitoring of employees, informing employees of filtering tools, use of logging systems, the appointment of privacy officers, and negotiation of the conditions of use of new technologies with workers' representatives. The CNIL also advocates the elaboration of corporate charters of computer system usage in the enterprise as a means of avoiding disputes between workers and employers.

The CNIL reports are merely advisory, however, and are not binding upon a French judge.

CONCLUSION

The net effect of the above laws can be summed up as follows: The "lien de subordination" which is inherent in the employer-employee relationship in France gives the employer certain prerogatives in regard to his employees - in particular the right to monitor in order to evaluate job performance.

Nevertheless, the employer must exercise these prerogatives while respecting the principles of "finalité", proportionality and transparency described in the applicable sections of the Labor Code.

Moreover, before putting into place any control or monitoring process, the employer must:

• inform its employees in a pro-active manner of the existence of monitoring or surveillance systems **- Article 121-8 of the Labour Code**

• declare the creation of databases containing personal data regarding its salaried employees to the CNIL

• consult the Works Council (if the company employs more than 50 people) prior to the introduction of "new technologies" into the workplace, when such technologies may have an impact on employment, remuneration, or other conditions of employment (Article L. 432-2, section 1) or prior to the implementation of any monitoring system (whether telephone, computer, or video surveillance) (Article L. 432-2-1, section 3). It is essential to note that the consequences of the employer's failure to adhere to the above requirements will be criminal sanctions, ie. fines and possible imprisonment.

The drafting of a "code of good conduct" for the use of the company IT system, while not yet mandatory for the employer, can place a company on the "good side" of the CNIL...

The drafting of a "code of good conduct" for the use of the company IT system, while not yet mandatory for the employer, can place a company on the "good side" of the CNIL and can generally assist in defusing uncertainty as to what is/is not acceptable behaviour on the part of the employee.

In summary, the law on workplace privacy in France, while currently evolving in favor of employees' rights in the recent case law, is still a moving target. A brief tour of the international horizon and notably a project of the European Commission for EU action in the field of protection of workers' data, may mean that the current unsettled state of the law will get worse, before it gets better.

AUTHOR: Nancy E Muenchinger is Avocat à la Cour and Attorney-at-Law at Paris-based law firm Denton Salès Vincent & Thomas. She can be contacted at Tel: +33 1 5305 1600 (ext 1692), E-mail: nmuenchinger@dentonwildesapte.com

FURTHER INFORMATION: For details on France's Labour Code, see the International Labour Organisation website at: www.ilo.org/public/english/employment/gems/eeo/law/france/l_lc.htm
Guidance on workplace privacy can be found on the CNIL's website at: www.cnil.fr/thematic/index.htm

Making the most of online privacy policies

Much more than just a legal requirement, your online privacy policy can bring a business boost to customer confidence. **Vanessa Smith Holburn** looks at the issues.

Pro-privacy groups such as Junkbusters ensure that issues of data protection are always in the news. Indeed, companies as large and as web-savvy as Amazon.com have found themselves on the wrong side of such organisations – unceremoniously hauled up in front of authorities like the US Federal Trade Commission (FTC) – rightly or wrongly - to explain procedures and policies covering the retention, use and transfer of customer details. Increasingly then, all companies must decide how best to handle the issue of privacy. To ignore the increasing transparency demanded by society surely runs the risk of a ruined reputation – and is a missed opportunity for brand loyalty.

"Consumers in the marketplace are much more aware of where their information is going and how it is being used, and I think that's driving consumers, more so than anything else, to read the [privacy] policy and look for some kind of trusted assurance."

- Mathew Ellis, Ernst & Young

Despite this new and intense focus on privacy policies, many companies still have room for improvement. A PA Consulting Group benchmarking study, published in June last year, revealed that while 74 per cent of the FTSE 100 websites studied gathered data on site visitors, over 50 per cent either had a privacy policy that the study rated as poor, or no privacy policy at all. In fact the results rated only 13 per cent of the companies as 'good' on their 'overall quality of privacy management'.

Likewise, six months ahead of the implementation of the revised EU Directive on Privacy and Electronic Communications a study carried out by KDB and Marketing UK found that while 97 per cent of UK top 500 companies posted a policy that brought it into compliance with current legislation, just 22 per cent offered an opt-in option for expressing marketing preferences.

ARE COMPANIES FAILING CONSUMERS?

The results of a Harris Interactive survey in February last year showed that consumers did not trust companies to handle personal information appropriately, with chief concerns being that data would be passed on to third parties without their permission, that hackers could retrieve their personal information and that online transactions were not secure. Shane Baylis, founder and managing director of KDB, says the KDB/Marketing UK results show that "companies are failing to recognise that consumer trust in e-business is faltering and the longer they postpone the inevitable, the worse the situation will become." He cites a recent KPMG report (see *PL&B UK*, May 2003, p.7) which suggests that data privacy is the consumer's greatest fear when shopping online and adds "this is simply not being addressed".

However, companies with an online presence need not see consumer anxieties over data protection as a problem. Matthew Ellis of Ernst & Young's privacy practice explains that a privacy policy is a communication tool which "gives organisations the ability to clearly communicate their procedures and the use of customer data to help set expectations with customers and employees that allows them…to make assurances that what they say they are doing, is what they are doing". In this way, in many cases the policy will serve as an introduction to the corporation for the consumer – and will affect how that customer goes forward to relate to the corporation's brand. He argues "privacy gives you the ability, again and again, to create products and services that will enhance customer [relations] without violating their privacy."

Interestingly though, while consumers report that they are worried about privacy, many confess that they do not read the available policies. A Harris Interactive poll undertaken in 2001 suggested that nearly 64 per cent of online shoppers either do not read, or skim through, a website's privacy policy. Likewise, Jupiter Research findings (June 2002) suggest that only 40 per cent of online consumers read such statements.

Nick McConnell, UK general manager of e-mail marketing firm Digital Impact, and chairman of the UK Direct Marketing Association's E-mail Marketing Council, says "I suspect very few people actually read these [privacy policies], although they are becoming savvy to the phrase 'share data with third parties', which suggests their personal data will be found on the open market."

But Ellis disagrees. He believes that the number of people reading privacy policies is growing because consumers

are becoming more aware of the issues around privacy, more technically savvy and because the media is increasingly communicating what can be considered as ideal standards and good practices. He argues "consumers in the marketplace are much more aware of where their information is going and how it is being used, and I think that's driving consumers, more so than anything else, to read the policy and look for some kind of trusted assurance." This is a view shared by Fran Maier, executive director of online privacy seal provider TRUSTe. She quotes a January 2003 BizRate survey which showed that 82 per cent of online shoppers have reviewed a privacy policy.

USE PRIVACY TO INCREASE CUSTOMER TRUST

Either way, if online privacy policies are viewed as an opportunity to build a relationship of trust with a customer base, rather than a chore (at a recent Deloitte & Touche European leadership forum, 70 per cent of e-business leaders believed that legal and regulatory hurdles hamper development), companies should look to encouraging all site visitors to access, read, understand and trust the published policy. This will ultimately transfer the trust achieved to the corporate brand. If privacy is of increasing public concern – and if at least a proportion of that public is reading the policies available – then it is high time organisations proactively used their policies effectively to build business, rather than just to maintain it.

In the past, online policies have been criticised for being too technical (indeed a *USA Today* article once suggested you need a PhD to understand some), too cluttered with legal jargon and too based on marketing and PR. Ellis explains "I think five years ago, privacy policies were much more technical than they are today, but I don't think leading company privacy policies are marketing or technically driven." He adds that if companies do not produce policies free from legalese and marketing "you're not going to build the level of trust you need to have that long-term customer."

Likewise, experts at retail technology solutions provider Hyperlink Interactive always recommend that clients "provide a straightforward policy that says what they will and won't do and provides clear access to the company in cases of doubt or concern." Client strategy director, Stephen Morris adds "my personal opinion is that it is far more important that the customer can understand the policy and feel comfortable about opting-in than for the policy to be a typical legal document." Like Ellis, he believes that the provision of clear privacy policies that demonstrate respectful behaviour to customer data "is essential for companies trading online – in terms of repeat business as well as customer service." He describes privacy policies as "a manifesto for the customer relationship."

> ...you can generate around 63 per cent more trust in your customers by using an independent auditing firm to verify that what you promise in your policy is really what happens

A POLICY TO HELP YOUR BUSINESS

But, alongside ensuring that your policy is accessible, how else can you ensure that your policy is working for both you and your customers? Maier recommends independent seal programmes like TRUSTe that can be seen to monitor sites – and act as a third party in disputes. Such endorsements can quickly amalgamate global legal requirements and evolve as the market needs. She says "58 per cent of online shoppers felt a non-profit, business or trade association was the best third party to ensure a company is honouring its privacy statement."

However, the systems are more often seen as a "step in the right direction" rather than a catchall, according to Deloitte & Touche's EU Data Privacy Coordinator Erik Luysterborg. Accordingly, Shane Baylis points out that the KDB survey results shows that self-regulation often doesn't work, even though he agrees regulators like TRUSTe can be effective.

Instead, Ellis tends towards deeper third party audit and verification, such as that earned from the AICPA (WebTrust), which gives the consumer "true assurance". He believes that having "a form of independent verification on that [your privacy policy] is a great trust enhancer." He also argues that you can generate around 63 per cent more trust in your customers by using an independent auditing firm to verify that what you promise in your policy is really what happens. If handled correctly, Ellis believes, privacy policies "should make a positive impact for both customer and organisation."

READ IT AND STICK TO IT

But Luysterborg warns your policy must be more than a page of text, is not just an issue of "ticking the box" and that it must act as a guide for the actual "back office infrastructure". He explains that "most of the companies who fell foul of data privacy regulations, did so not merely because they did not have data privacy policies…but because they had not acted in accordance with them." He adds "you need to adopt a coordinated and pragmatic corporate approach and work out a plan to apply to your particular organisation's processing and transfer of data." Avoid a "paper tiger syndrome" he warns, which serves to lull companies into a false sense of security, believing that legal safety is simply obtained by putting a data privacy policy on display. Instead, he argues that policies should be ever changing, and that a one-size-fits-all formula cannot work. Perhaps then, it is companies themselves who have most to gain by reading their own policies?

AUTHOR: Vanessa Smith Holburn is a freelance journalist specialising in IT and new media law.

Your Newsletter Subscription **Includes**

1. Five Newsletters a year
The *Privacy Laws & Business* 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 UK/International newsletter

❑ Yes, I will subscribe to the *Privacy Laws & Business* International Newsletter. Subscription: £325/$520/Eur 490

❑ Yes, I will subscribe to both the *Privacy Laws & Business* International and UK Newsletters. Combined discounted subscription: £520/$830/Eur 780

❑ Yes, I already subscribe to the *Privacy Laws & Business* UK Newsletter. I would now like an additional subscription to the International newsletter: £270/$430/Eur 400

❑ I do not wish to receive the free e-mail update service as part of my subscription.

❑ Yes, I am interested in subscribing to the *Privacy Laws & Business* International Newsletter in PDF format. I would need ..... sites to access the newsletter on our Intranet or network. (We will call you to discuss licensing).

❑ Yes, I wish to receive discounted multiple copies of this newsletter. Please write number required .....

Data Protection Notice: *Privacy Laws & Business* will not pass your contact details to others without your consent. Please indicate if you do *not* wish to receive further information about:
❑ our recruitment service ❑ our other products and services.

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel: Fax:

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 17/06/03

www.privacylaws.com

Guarantee

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