News in brief

WORKPLACE PRIVACY

A Danish High Court has ruled in favour of an employee who was sacked for sending hundreds of personal e-mails and visiting a sex-chat site. According to law firm Baker & McKenzie, the company, Salut Audio & Video ApS, did not have an e-mail and Internet staff policy and failed to provide the employee with a warning before dismissal. A city court had previously upheld the dismissal as being justified.

The UK has introduced equal pay regulations allowing employees to find out the salaries of fellow workers. Lawyers have warned that this could conflict with the UK's Data Protection Act. *See the May issue of PL&B UK for the full story.*

An Australian federal government employee has won AUS$7,000 (around €4,000) in compensation after his employers breached the National Privacy Principles by passing on sensitive medical information to a panel that was interviewing him for another position.

The French Data Protection Authority has issued a statement reminding employers of their obligations during the recruitment process. Employers should not record sensitive personal data (racial origin, political or religious beliefs etc.) without candidates' consent. Potential employees should also be informed if automated decision taking is used, and of their right to access their details.

US hackers apparently attempted to extort money from over 30 office workers by planting pornography on their computers. They then blackmailed the hapless employees by threatening to inform their supervisors. Fear of dismissal caused some to pay up and hand over their credit card details. *See the full story at: www.idg.net/ic_1145409_9676_1-5122.html*

Most EU consumers read privacy policies

A new survey from the University of Tilburg in the Netherlands has shed some light on the privacy preferences of European consumers. The survey, *Building Consumer Value through the Internet*, gauged the opinion of over 62,000 web users from 146 countries. Around 94 per cent of the respondents were based in the EU, with the majority coming from the UK, Germany, the Netherlands, Italy, and France.

The survey revealed that 65 per cent of online consumers do examine privacy or data protection statements when visiting commercial websites that collect personal data. Of greatest concern (39 per cent of respondents) is whether the website will share or sell their details onto other companies. 32 per cent want access to their accounts so that they can change their details, either to personalise their accounts or rectify inaccurate data.

Less high up on the list of priorities (28 per cent), although still significant, is whether the website has "trust marks", such as certification schemes provided by consumer groups or direct marketing associations. Finally, 24 per cent of consumers will look to see if the website they visit limits the collection of excessive or unnecessary data.

On the security front, 56 per cent of respondents indicated that they were not confident about shopping online. 27 per cent, however, said that they were confident, provided that the website posted an explicit security statement. Only 17 per cent expressed full confidence in online shopping.

Further information: www.tilburguniversity.nl

France's Senate approves data protection bill

On April 1st, France's Senate (upper house) approved a new data protection bill that will update the existing 1978 law and bring the country into line with the rest of the European Union. France and Ireland are the only two remaining EU member states that are yet to transpose the EU Data Protection Directive into national law.

France's National Data Protection Authority (CNIL) has stressed that many aspects of the current law will remain unchanged, suggesting that it is more a case of modernising the existing regulations as opposed to a radical upheaval of the law.

However, there will be some significant changes to the current 1978 law. The bill proposes to grant the CNIL strengthened enforcement powers. New sanctions will include the right to levy fines of up to €300,000. Currently, the CNIL is restricted to issuing warning notices and referring cases of non-compliance onto the courts. The CNIL will also be given increased powers to carry out on-site data protection audits.

Private sector organisations which process specific categories of sensitive data (for example, genetic data, criminal records, or adverse credit information) will need to obtain prior authorisation from the CNIL.

The bill, which was originally adopted by the National Assembly in January last year, did contain some amendments made by the Senate. One amendment involves allowing medical research companies to make use of anonymised personal data, which will be subject to approval by the CNIL.

The bill will now be passed back to the National Assembly and could be finalised as early as this summer.

See PL&B Int, September 2002, p.10 for previous coverage on French data protection.

US marketers rally against 'do-not-call list'

The US telemarketing industry is bracing itself for tough times ahead after the creation of a nationwide telephone preference service which received presidential approval on March 11th.

The so-called 'do-not-call list' is to be officially launched on July 1st, allowing consumers to opt-out from receiving telemarketing calls by registering on a list that will be managed by the Federal Trade Commission (FTC). Marketers will be required to screen their databases against the list every three months and are not permitted to contact anyone on the list for a five-year period. Fines for non-compliance could reach up to $11,000 per violation.

The FTC has proposed a yearly fee of $7,250 for access to the list (marketers have until May to respond to the proposals), which will help contribute towards the $16 million first year budget of running the service.

There are exemptions to the list, but they are few - charities, market researchers, businesses who have an existing relationship with customers on the list (within the last 18 months) and, of course, politicians.

Pro-marketing groups question whether the list is actually needed. Currently, there are 26 states operating separate do-not-call lists. Pennsylvania, for example, already has 2.6 million people registered on its list. Additionally, there is the telephone preference service operated by the Direct Marketing Association (DMA). It states that 7.5 million consumers have registered on its list and claims an 80.5 per cent success rate in suppressing unwanted calls.

Statistics as to the size of the telemarketing industry and the impact of the new legislation depends upon who you speak to. The DMA says the industry employs four million people and generated $275 billion in 2001. The American Teleservices Association (ATA), however, estimates annual revenue to be as high as $660 billion. According to the ATA, government estimates suggest that the marketing industry could face losing 60 per cent of that figure.

Jason Catlett, president of consumer group Junkbusters, suggests that the figures have been somewhat overinflated. "Telemarketing is an idea whose time has gone. This line of business should just die quietly. Their ridiculously inflated figures claiming that the average American gives a thousand dollars a year to telemarketers just don't pass the smell test."

The marketing industry is not going down without a fight, however, and is making last ditch attempts to salvage some sort of lifeline. In January, the DMA and the ATA filed two separate lawsuits against the FTC, claiming the list to be unconstitutional and an infringement on their first amendment right to advertise.

Matt Mattingley, director of government affairs at the ATA, is confident that his organisation's suit will be successful. In a statement made in January he said: "Any attempt to restrict free speech places a significant burden on government to justify its actions. The FTC has failed to meet that burden. We believe their proposal will not withstand legal scrutiny."

That opinion, however, is not shared by everyone. In late March, a federal judge involved in one of the lawsuits said: "The Court finds the plaintiffs have failed to show a substantial likelihood that they will prevail."

He also warned that they would not be able to delay the implementation of the do-not-call list by carrying on with the suit.

Junkbusters' Catlett takes a similar line to the judge's statement: "Their first amendment claims have been repeatedly rejected by courts in other analogous cases such as junk faxes. The suits are simply a desperate delaying of the overdue."

Further information:
For details on the do-not-call list: www.ftc.gov/bcp/conline/edcams/donotcall/index.html

ACLU admits privacy blunder

Accidental privacy breaches are a nightmare for any organisation, but when one of its goals is to push for better privacy protection, then the embarrassment becomes ten-fold.

Towards the end of February, the American Civil Liberties Union (ACLU) admitted it had exposed around 850 e-mail addresses when sending out its ironically titled "Safe & Free" e-newsletter.

And this is not the first privacy blunder to beset the ACLU. In January this year, it agreed to pay out $10,000 in a settlement with the New York State Attorney General's office. It appears that the ACLU had exposed around 90 customers' names, postal and e-mail addresses, and purchase histories via a search facility on its website.

What makes the recent incident even more embarrassing is the fact that the ACLU had previously taken the moral high ground when US pharmaceutical company Eli Lilly became a victim of the same type of breach (*PL&B Int*, Feb 2002, p.10). In this particular case, Eli Lilly had exposed around 700 customers signed up to a prescription reminder service. An employee had accidentally placed recipients' addresses into the 'To:' line of the e-mail instead of the 'Bcc:' line (blind carbon copy).

Barry Steinhardt, associate director of the ACLU, had lambasted Eli Lilly's settlement with the Federal Trade Commission in January 2002, calling for stiffer financial penalties and suggesting there should be a "price to pay for being careless with highly sensitive information."

Steinhardt was certainly right to point out that Eli Lilly had exposed sensitive personal data. But by the same token, his organisation has done the same thing by revealing individuals' political affiliations.

Jim Harper, editor of web-based think tank, Privacilla.org, summed it up when he spoke to *Fox News*: "They really are throwing stones at glass houses. They took a holier-than-thou attitude and then turned around and did the same thing."

Hong Kong e-commerce stifled by lack of privacy

Raymond Tang, the Privacy Commissioner for Hong Kong, has said that the e-business community needs to take a more proactive approach to privacy. In his annual report for 2001-02, Tang said, "it is the absence of control that explains why consumer expenditure online remains such a very small percentage of total customer expenditure. Survey after survey show that consumers in Hong Kong want to control their personal data just as they want to control their personal expenditure."

Tang expressed regret that IT vendors appear to be more concerned about creating technology to track and profile people on the Internet than developing tools to protect customers. He suggested that the technology community develop "e-vendor" codes of conduct on the protection of personal data privacy.

The Commissioner's annual report showed that complaints have risen to 888 over 2001-02, a 12 per cent rise from the previous year. Many of the cases were either unsubstantiated or resolved through mediation. 48 cases led to formal investigations with 20 resulting in a warning or enforcement notice being issued. The majority of complaints (68 per cent) concerned the private sector, with financial services, telecoms, and property management the most likely source of complaint.

Tang cited notable improvements in compliance with the code of practice on human resources, which came into effect in April 2001. A previous area of concern had been the collection of personal data through recruitment advertisements in which the identity of the company soliciting the information was not disclosed. An investigation prior to the publication of the code revealed that 25 per cent of advertisements were failing to disclose the identity of the advertiser. However, in 2001-02 that figure was reduced to around 12 per cent.

Other initiatives during 2002 included draft codes on employee monitoring in the workplace and the provision of telecoms services. There was also a revision of the consumer credit code which increased data retention periods and the scope of use for credit data, and also built in additional safeguards.

Further information:
www.pco.org.hk/english/publications

Canadian businesses failing on privacy practices

In his 2001-02 annual report, Canada's Federal Privacy Commissioner, George Radwanski, gave cautious praise to organisations attempting to adjust to the Personal Information Protection and Electronic Documents Act (PIPEDA) during its infant years. At the same time, the Commissioner identified several systemic problems. Among the failings of organisations subject to the act were the following:

• being "less than thorough" about putting privacy codes into practice

• failing to designate a privacy officer, as required by the act

• not knowing how to process access requests and complaints

• keeping information too long or not long enough (one organisation did not destroy any personal information it collected because it did not know it was allowed to)

• failing to meet the 30-day limit on providing access to individuals, generally due to inefficient procedures rather than deliberate intransigence

• not limiting the information collected to that which was necessary

• not identifying the purpose for which the information was being collected

• failing to implement adequate informational safeguards; and

• not recognising that employees also have privacy rights.

Banks accounted for 45 per cent of the complaints under the act between January 1st and December 31st 2001. Telecoms and broadcasting organisations accounted for 28 per cent, and transportation organisations accounted for 18 per cent. The high percentage of complaints relating to these sectors reflects the limited range of organisations to which the act applies at this time. Provincially-regulated organisations - apart from those in Quebec, which are already covered by provincial legislation - are not covered by the federal act until 2004.

The annual report also explained the Commissioner's interpretation of the act. In particular, he noted: "There has been considerable progress made in interpreting what is and what is not personal information...I am inclined to regard information as personal even if there is the smallest potential for it to be about an identifiable individual."

Even so, Radwanski concluded, a deliberately broad definition must have limits. Specifically, he decided that physicians' prescriptions or prescribing patterns did not constitute personal information about physicians themselves. An individual prescription, he concluded, is potentially revealing information about a patient, but it is not in any meaningful sense about the prescribing physician as an individual.

Despite the deficiencies noted by the Commissioner, he found it encouraging that, once systemic problems had been pointed out to them, organisations "by and large" were quick to accept and implement the recommended remedies.

Further information:
www.privcom.gc.ca/information/ar/02_04_10_02_e.asp