



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 intro-

duced 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.