global privacy roundup

AUSTRALIA

Karen Curtis has been appointed as Australia's new Federal Privacy Commissioner. Curtis was previously director of industry policy for the Australian Chamber of Commerce and Industry (ACCI).

TV broadcasting company, Seven Networks, has won a landmark privacy ruling after it accused a trade union of breaching the privacy rights of its employees.

The Federal Court ruled that the trade union had breached the Federal Privacy Act by making unauthorised use of Seven's internal employee directory, which was used to poll staff opinion on a new enterprise agreement being proposed by Seven. See the full report on p.12.

CANADA

The Privacy Commissioner for British Columbia has launched an investigation into the outsourcing of personal data by public sector organisations to US-based service providers.

The investigation centres around the privacy implications that might arise as a result of US government authorities accessing outsourced data under the US Patriot Act, which was passed shortly after the September 11th attacks in 2001.

The Commissioner, David Loukidelis, has said that the investigation will focus on whether US authorities are able to access data on British Columbian citizens, under what conditions this could occur, and what steps could be taken to mitigate the privacy risks. [see cover story for more details]

The Federal Privacy Commissioner for Canada has earmarked CAN$200,000 for research and promotion of privacy protection. The intention behind the funding is to examine two key areas. The first is the privacy impact of surveillance technologies such as video surveillance, radio frequency identification devices (RFIDs), location technology, and biometrics. The second area is research into the implementation of Canada's Federal privacy law (the Personal Information Protection and Electronic Documents Act (PIPEDA)) which was extended to cover all private sector organisations in January 2004. For further details see: www.privcom.gc.ca/media/nr-c_e.asp

FRANCE

The national data protection authority (CNIL) has stated that businesses will no longer need to declare payroll processing activities with the regulator. The announcement, made in June, preempts the introduction of amendments to the existing data protection law which aim to simplify the procedures for registering data processing operations with the CNIL. The amendments, which will bring France's data privacy law in line with the EU Data Protection Directive, is expected to be passed by the end of September this year.

Another of the simplification provisions proposed in the French bill includes exempting registration or notification with the CNIL for organisations that appoint a dedicated data protection officer. See p.17 for more details.

GERMANY

On June 2nd, the Federal Data Protection Commissioner for Germany, Peter Schaar, issued a statement on the use of 'reverse searching' in telecoms directories. Reverse searching is a practice used by marketers to obtain the names and addresses of potential consumers by keying in random telephone numbers into directory search engines. Schaar stated that once Germany's implementation of the E-privacy Directive comes into force (expected this year), telecoms services providers will be required to allow customers to opt-out from having their directory details made accessible by reverse searching methods. Schaar added that customers must be clearly informed about the right to opt-out and have the opportunity to withdraw their consent at any time.

INDIA

While the debate continues on what steps the new Indian government will take to regulate data protection compliance (*PL&B International*, March/April 2004, p.1), industry group NASSCOM is planning to introduce self-regulatory measures to restore confidence in the outsourcing sector. According to *Rediff.com,* NASSCOM wants to set up an industry certification body to ensure Indian-based service providers implement adequate security procedures. The group has also launched a 'Trusted Sourcing' initiative with market intelligence group Evaluserve, to assess the level of security compliance in the Indian IT sector.

In May, the Reserve Bank of India issued a directive to financial services providers warning them over the use of customer details to cross-sell third party products and services. The Reserve Bank has expressed concern that banks are breaching customer confidentiality by passing on personal data to third parties without their consent.

The Reserve Bank has stipulated that any information collected when customers open their accounts cannot be passed on to third parties. Banks are permitted to collect the same details separately if customers are given notice on how their data will be used and they have given their "express" consent.

JAPAN

The Financial Services Agency has criticised the Japanese branch of Citibank after it lost data on around 125,000 ATM, credit card and investment transactions. According to the *Associated Press*, the Financial Services Agency has criticised Citibank for delays in notifying customers and the agency about the incident. The bank has now been given until July 12th to submit a plan to the agency detailing the steps it will take to improve security and privacy compliance.

Two men were arrested in June in connection with the theft of personal data belonging to four and a half million customers of Internet service provider Yahoo! BB, a joint venture between Softbank and Yahoo!

The two men allegedly attempted to extort up to $18 million from Softbank, threatening to publicly release the customer details which included names, postal and e-mail addresses, and phone numbers.

KOREA

South Korea looks set to implement additional public sector privacy legislation next year after the cabinet approved a draft bill prepared by the Ministry of Government Administration and Home Affairs in early June. Korea has already implemented the Protection of Personal Information Act for public sector bodies, but there have been concerns over the amount of personal data that can be collected and shared between public agencies. According to the *JoongAng Daily*, the proposed law would limit data sharing and collection, although there is likely to be exemptions drafted in for national security, criminal matters and tax audits.

NETHERLANDS

Towards the end of April, the Upper House of the Dutch Parliament approved a spam bill which will implement the EU Privacy & Electronic Communications Directive. The Netherlands is one of several EU member states facing legal action for failure to meet the October 2003 transposition deadline (other countries include Belgium, Germany, Greece, France, and Luxembourg).

However, the Netherlands may escape legal action if the bill is introduced this summer. The new law will require marketers to obtain prior consent from consumers before sending out e-mail, SMS or fax advertising. However, the rules will apply to individuals only - business subscribers will not be afforded the same level of protection. According to *DMeurope*, the Dutch Telecoms regulator, OPTA, will be responsible for enforcing the new law.

TAIWAN

In May, the Democratic Progressive Party (DDP) published a draft amendment to Taiwan's current privacy law, the Computer-Processed Personal Data Protection Law. According to the *Taipei Times*, the intention is for the law to be renamed the 'Personal Protection Law' as the scope of its powers will be extended to cover manual/paper-based information. The draft amendment proposes criminal penalties including up to seven years in prison and/or a fine of up to TWD$40,000 (US$1,200; €1,000).

There are also proposals to extend the scope of the law to all organisations that process personal data - currently the law only applies to specific sectors such as telecoms, finance, healthcare etc.

The amendments could be set before the legislature this autumn.

UNITED KINGDOM

New regulations on unsolicited telemarketing calls to businesses come into force on June 25th. The regulations will establish a do-not-call registry allowing businesses to opt-out from unwanted marketing calls. Telemarketers that break the regulations by failing to screen their databases against the registry can receive a maximum fine of £5,000 (€7,500, $13,800).

Businesses will be able to register telephone numbers onto the new corporate telephone preference service on an annual basis, but will be required to submit their requests in writing in order to avoid possible fraud.

The Information Commissioner's office has published guidance on the new rules, available at: www.informationcommissioner.gov.uk

The National Consumer Council (NCC) has published a report into the privacy implications of RFID (radio frequency identification) tracking tags.

The report calls for industry to act quickly to implement privacy safeguards, engage with consumers to build up public trust in the technology and provide convincing evidence of the benefits of RFIDs.

An action plan drawn up by the NCC has recommended government research into the legal implications, consumer research, and industry-government consultation on how to proceed. For a copy of the report: www.ncc.org.uk/technology/rfid.pdf

UNITED STATES

A new privacy law comes into force in California on July 1st. The Online Privacy Protection Act, will require any online business that collects personal data from customers residing in California to post a privacy policy. The policy must include details on what types of personal data are collected, what types of third parties the data may be shared with, and whether customers can access or request changes to their records.

Companies whose practices conflict with their privacy policies will be in breach of the law. Businesses that fail to post a policy will be given a thirty day period to publish a policy once they have been informed that they are non-compliant.

In late May, the Californian Senate passed a bill on monitoring in the workplace. SB 1841 is intended to update existing state labour law on the interception and monitoring of phone calls to cover Internet and e-mail usage. The bill does not argue for a ban on monitoring, but proposes that employers be required to inform staff whether they intend to read their e-mails or track Internet usage.

The bill has now been passed over to the Californian Assembly.