INTERNATIONAL newsletter
ISSUE NO 61 FEBRUARY 2002

Editor & Publisher
Stewart H. Dresner
Tel: +44 (0)20 8423 1300
stewart@privacylaws.com

Associate Editor
Eugene Oscapella
eugene@privacylaws.com

News Editor/Assistant Editor
Alan Pedersen
Tel: +44 (0)20 8423 1300
alan@privacylaws.com

Newsletter Subscriptions
Gill Ehrlich
Tel: +44 (0)20 8423 1300
gill@privacylaws.com

Issue 61 Contributors
Professor Joel Reidenberg

Contributions
Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items for consideration, contact: alan@privacylaws.com

Published by
Privacy Laws & Business,
5th Floor, Raebarn House,
100 Northolt Road,
Harrow, Middx HA2 0BX, UK
Tel: +44 (0)20 8423 1300
Fax: +44 (0)20 8423 4536
internet: 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. Whilst 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 Triumph Press +44 (0)20 8951 3883

ISSN 0953-6795

privacy news

EU adopts further measures for overseas data transfers

On 23rd January, the European Commission adopted a decision aimed at simplifying the transfer of personal data to processors in non-EEA (European Economic Area) countries.

The Commission's standard contractual clauses will allow businesses to transfer personal data, such as customer information, to subcontracted processors in countries which are not recognised by the EU as offering an "adequate level" of protection. The clauses will require companies to ensure that the recipients of their information treat it in accordance with the EU Data Protection Directive.

The decision is an extension of the existing clauses, which previously allowed the transfer of information only to data controllers. The clauses are not compulsory and are one of a number of possibilities for lawfully transferring personal data. However, the advantage of using the standard contractual clauses is that EU Member States' Data Protection Authorities are obliged to recognise the transfer process as compliant with the Commission's Directive (PL&B Int, Sep 01 p. 3).

US firms still steering clear of Safe Harbor

Speculation that Microsoft's adoption (in June 2001) of the Safe Harbor principles (required to facilitate the import of personal data from EU countries) would stimulate much greater interest from US businesses – has proved unwarranted. Since the Safe Harbor was set up in July 2000, only 154 companies have so far signed up.

For more information and analysis of the Safe Harbor agreement, see PL&B Int, May 01 p.6.

China cracks down on subversive web content

According to an Associated Press report, the Chinese Ministry of Information Industry is tightening its grip on its citizens by increasing its control over the Internet. The ministry has ordered ISPs to monitor and forward to the authorities any e-mail traffic that contains politically sensitive material. They will also be required to delete any subversive or prohibited material hosted on their sites.

Furthermore, foreign software developers such as Microsoft, who export their products to China, will be required to sign undertakings that their products are free of any spying or hacking software that could compromise national security.

For more information on China, see PL&B Int, Jan 02 p.11

Qwest backs down over information sharing

On January 28th, following a flood of complaints from customers and pressure from US senators, telecoms operator Qwest withdrew its plans to share client data with its subsidiary companies. US Senator Paul Wellstone had previously urged the Federal Communications Commission (FCC) to force Qwest into changing its privacy policy. Customers were required to read and accept a detailed and complicated "opt out" policy in order to stop personal data being passed on to Qwest's subsidiaries. In its defence, Qwest said that only "appropriate" information will be sent out, and that consent is obtained should it wish to send data outside the company and its affiliated partners.

The announcement is likely to ease demands for Qwest to revert back to the "opt in" policy which was "invalidated" in 1999 after an appeal by telecoms operator US West. US West and Qwest merged in 2000.

New Laws

Canada: Ontario announces development of data protection draft legislation

The Ontario government has announced that it is developing draft privacy legislation aimed at creating a comprehensive approach to privacy protection in the province.

Like Canada's federal private sector data protection legislation, the Personal Information Protection and Electronic Documents Act, the proposed Ontario legislation is based on the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information. That code contains 10 privacy principles that have been adopted as a voluntary national standard (PL&B Int, Sep 96 p.8-10).

Currently, Canada's federal law generally only applies to activities falling within the jurisdiction of the federal government. The Act's privacy protections will extend to the provinces and territories by 2004, unless they enact "substantially similar" legislation before then. The proposed Ontario legislation is clearly intended to avoid the extension of the federal legislation to cover commercial activities that would normally be regulated by the Ontario government. The Ontario government is requesting comments by March 8th 2002 on its consultation paper describing the proposed legislation.

Ontario legislature enacts controversial blood test law

Canada's *National Post* newspaper reported on December 15th 2001 that the Ontario Legislature had pushed through controversial legislation requiring individuals to give blood samples to protect victims of crime, emergency workers and 'good Samaritans'. The *Health Protection and Promotion Amendment Act 2001*, is the first of its kind in Canada, and received almost unanimous support in the Legislature when it was passed before Christmas.

Under the law, emergency workers can demand that the people they help provide blood samples to be analysed for AIDS, Tuberculosis, Hepatitis C and other communicable diseases. Anyone rescued by a 'good Samaritan' could be forced by the law to undergo blood tests, as could individuals accused of assault, even if they have not yet been convicted. Until now, there was no way to force such testing.

The test results will be given to the applicant, turning a longstanding rule of medical confidentiality on its head. A police spokesman argued that the test results will reduce the number of cases where emergency personnel have to take preventative drug treatments with their many side effects.

The province's own chief medical officer of health was harshly critical of the legislation when he reviewed it before a committee in early January. "The legal and ethical rules of sound public health practice respecting confidentiality and privacy issues involving patients are ignored under the bill," he said. He went on to say that there were no documented cases in Ontario of the transmission of these diseases to emergency workers.

The president of the Ontario Medical Association was equally troubled. He was concerned that health information that has always been subject to patient-doctor confidentiality will now be shared with emergency workers, good Samaritans and victims of crime.

Further information:
www.ontla.on.ca/library/bills/105372.htm
www.nationalpost.com

Personnel Moves

UK Information Commissioner to step down

Elizabeth France is quitting her position in November as the UK's Information Commissioner when her contract expires. The decision follows reported conflicts between Mrs France and David Blunkett, the Home Secretary, over the introduction of the government's Anti-Terrorism legislation and its impact on civil liberties and personal privacy.

Mrs France's position has now been advertised and can be found at: www.lcd.gov.uk/foi/

Danish DP Agency appoints acting head

Lena Andersen has been appointed to the position of Acting Managing Director of the Danish Data Protection Agency. She temporarily replaces Henrik Waaben, who will be an acting High Court Judge until April 30th 2002.

The DPA has also changed its name from 'Registertilsynet' to 'Datatilsynet' (PL&B Int, Jan 02 p.12 for more details).

The new contact details are:
Datatilsynet
Borgergade 28, 5th Floor
DK 1300 Copenhagen K
Phone: +45 3319 3200
Fax: +45 3319 3218
E-Mail: dt@datatilsynet.dk
www.datatilsynet.dk

Guernsey update

Dr. Peter Harris has been appointed as Guernsey's first full-time Data Protection Commissioner. He replaced Winston Bull, who undertook the role on a part time basis, on October 1st 2001 (see PL&B Int, Jan 02 p.16 for more details).

The Data Protection Commissioner can be contacted at:
P.O. Box 43, St. Peter Port
Guernsey, GY1 1FH
Tel: +44 (01481) 717007
Fax: +44(01481) 712520
www.dataprotection.gov.gg

Privacy vital for CRM Initiatives

US Companies who use Customer Relationship Management (CRM) software will have to place more emphasis on privacy, according to a report published on January 7th 2002 by technology analysts Gartner. Impending legislation and growing customer demand is forcing companies to invest in new systems – or build on existing solutions – that allow more pesonalisation of privacy. According to Gartner, 40 per cent of US firms that have already installed CRM solutions will be rethinking their strategies.

Australia publishes PKI guidelines for government agencies

In an effort to enhance communication between government agencies and the public, the Privacy Commissioner has published guidelines for the use of Public Key Infrastructure (PKI). With Internet usage on the rise, there is a growing demand for online services, prompting the need to ensure that privacy is maintained and communications channels are secured.

Public Key Technology is an electronic form of encryption using public and private keys to ensure the secure transfer of data. PKI refers to the encryption infrastructure that an organisation uses, covering the types of technology used, the privacy policies adopted, and the management of these systems.

There are a number of privacy enhancing benefits in using PKI. It reduces the need to disclose personal information in order to identify a user, opens up more channels for communication, and offers a safe and more secure alternative to some existing channels.

But whilst Privacy Commissioner, Malcolm Crompton, acknowledges the benefits of using PKI, he believes that guidelines are necessary in order to combat the potential risks involved in setting up these systems. Concerns have been raised over a number of issues, including security breaches, tracing online transactions, and using public key databases for individual profiling.

A review of government agencies' implementation of PKI will begin in eighteen month's time, during which the private sector's use of PKI will also be monitored with a view to introducing further legislation at a later date.

Details of the guidance can be found at: www.privacy.gov.au/government/guidelines/index.html#1

Australia: laptop thefts pose security risks for government

On January 16th the Australian online news service *Australian IT* reported claims by federal opposition politicians that highly classified defence and cabinet information could have been compromised by the theft and loss of more than 500 government laptop computers over the last year. One opposition spokesperson claimed that the Defence Department alone was unable to account for 127 laptops in the 1999-2000 financial year. Several departments have reportedly refused to respond to opposition queries about the alleged losses.

For further information: www.australianit.news.com.au/articles/0,7204,3601071^15319^^nbv^15306,00.html.

Surveillance technology: Blushing liars

Results of research for discovering better means of detecting liars has just been published in the United States. It seems shifty eyes are no longer the issue, but rather the heat generated around those same eyes when liars involuntarily blush.

The *Toronto Globe and Mail* (January 3rd) reported that US researchers claimed they had been able to detect lying in three quarters of the people they tested and over 90 per cent of others telling the truth through the use of a high-definition heat-sensing camera. The technology may one day be used for evaluating people's responses to questions such as: "Did you pack your own bags?" or "Why did you enter this facility?" The technique measures the face's "thermal signature" and detects an invisible heat blush around the eyes that is thought to be produced when people are lying.

The newspaper reports that, while the technology was originally funded as a project seeking to improve the detection of spies at US defence facilities, it is now promoted as a terrorist-thwarting method in more public venues. The success rate is reportedly similar to the accuracy of traditional lie-detection (polygraph) tests, which have a less than stellar track record - as low as 49 per cent accuracy in some cases; although the accuracy rates reported in a recent review of 11 polygraph studies averaged 71 per cent.

The technology appears to be far from ready for the rough and tumble of widespread use in the business sector. Given the enthusiasm in some jurisdictions for ensuring employee honesty, will the "blush test" work its way (with the accompanying controversy) onto the employment scene?

Surveillance: Big Brother is leering at you

The editors of *Scientific American* remark in their December 2001 issue that the talk today is of more, rather than less, surveillance. Instead of "Big Brother is watching you," we hear "Big Brother is watching out for you."

The editors pause to question the security technology that is increasingly being suggested as an important element of the solution to tackling terrorism. The editors ask two questions: First, how well does the technology really work? It refers to a US Defence Department study that found even the best facial recognition camera systems "choke" when the setting changes just slightly from the setting of the digitised picture that underlies the technology.

Second, the editors ask, what is the technology really being used for? They cite findings of a recent UK study by University of Hull criminologists on the use of security cameras that "the young, the male and the black are systematically and disproportionately targeted... for no obvious reason." The editors further suggest that "walking while female" was another 'offence' that drew camera operators' attention. Those who favour surveillance technology, they argue, may be less enthusiastic when they learn that the technology is more often used to track petty crooks or even innocent citizens than potential terrorists; even if the technology has the potential to be effective, too

often its human operators attempt to pervert its application.

The editors propose a solution. If cameras are to be tried, enact time limits or sunset provisions. The cameras come down and the databases are erased after a specified period, unless electors vote otherwise. "That way, society can experiment with security cameras without risking a slide towards a surveillance state."

Casablanca revisited: A kiss is just (not) a kiss, a scam is just a scam

Online news service, *Newsbytes*, reported January 16th on an Internet scam sure to take the fun out of Valentine's Day. Authorities have moved to shut down the latest "InstaKiss" website designed to dupe American Online (AOL) users into disclosing their account passwords in exchange for an electronic kiss.

Newsbytes claimed that the operator of the latest password-stealing site sent a bogus invitation to AOL users by instant message and e-mail. The message informed recipients that they had been sent an "AOL InstaKiss" by "someone who thinks very highly of you." By clicking a link in the message, the AOL user could receive his or her InstaKiss.

The site to which the link connects, bore the AOL logo and instructed visitors to type in their AOL screen name and password to receive their InstaKiss.

For further information: www.newsbytes.com/news/02/173689.html

Security concerns over proposal for United Kingdom e-voting scheme

Critics have expressed concern over plans by the leader of the House of Commons, Robin Cook, to bring in voting on the Internet in time for the next general election, according to a Guardian report dated January 7th. The newspaper reports that local pilot schemes are already in place for electronic voting in this year's local elections. Critics, however, argue that there are legitimate questions about the security of Internet voting. The report mentions that only one country now votes online – Estonia.

For further information: www.politics.guardian.co.uk