INTERNATIONAL newsletter
ISSUE NO 62 APRIL 2002

Editor & Publisher
Stewart H Dresner
stewart@privacylaws.com

Associate Editor
Eugene Oscapella

News Editor
Alan Pedersen
alan@privacylaws.com

Newsletter Subscriptions
Gill Ehrlich
gill@privacylaws.com

Issue 62 Contributors
Judith A Sullivan
Gary Brooks
Merrill Dresner
Francis J Kean
Tom Lenon
David Goldberg

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

Laws and regulation

Spain's DPA imposes 12 million euros in fines during 2001

The Spanish Data Protection Agency (APD) revealed that it has imposed substantial fines on Spanish businesses which fail to comply with data protection laws. Speaking at an event on data protection in the financial sector in March, the APD's director, Juan Manuel Fernandez, said that a total of 12.02 million euros had been levied across 500 separate cases during 2001. The APD examined a number of areas in e-commerce, including insurance, electronic banking, and loyalty card schemes organised by supermarkets and department stores.

Hong Kong presses ahead with digital identity cards

The *New York Times* reported on February 15th 2002 that Hong Kong plans to update its decades-old identity card system. The new card would contain a computer chip with a digital replica of the cardholder's thumbprint.

Hong Kong currently requires all residents aged 11 or older to carry a card. Sin Chung-Kai, a pro-democracy member of Hong Kong's legislature, said: "We're not opposed to people having to carry ID cards. The crux of the controversy is how much other information about a person should be stored on the card." Hong Kong's current ID has a photograph, biographical data and the cardholder's residency status. The *New York Times* reported that the new card's chip has the capacity to include much more information, including medical and financial data, and driving records.

Reuters news agency reported on February 26th 2002 that the Hong Kong government had awarded a contract for the initial delivery of 1.2 million smart cards, in addition to hardware, software and services for the new system.

See page 14 for interview with the Hong Kong Privacy Commissioner

New Irish data protection rules come into force

New regulations partially implementing the EU Data Protection Directive came into effect on April 1st. The European Communities (Data Protection) Regulations 2001, adopt four articles from the EU Data Protection Directive. They cover the transfer of personal data to countries outside the European Economic Area (EEA), security measures that organisations must have in place in order to protect personal data, contracts for third party "data processors", and a reworking of the application of the Data Protection Act to foreign data controllers.

Tom Maguire, the Deputy Data Protection Commissioner, told *PL&B International* that further implementation of the EU directive would "require legislation to be passed by Parliament, which hopefully will occur in the next few months." He stressed, however, that due to the upcoming election, the proposed bill on data protection could be delayed until later in the year.

For more information, see the Commissioner's website at: www.dataprivacy.ie

The dangers of baring one's (er) soul in public

A Florida State University student who bared her breasts at Mardi Gras in New Orleans has sued the producer of the *Girls Gone Wild* video, contending that her privacy was invaded and that the producer used her image without her permission. The lawyer for the producer argues

©2002 Privacy Laws & Business

that there is no right to privacy for people who strip in public in front of thousands of revellers.

Technology

E-mail security – an object lesson

The Economist magazine reported on February 23rd 2002 that a security breach involving an e-mail from the European Union's ambassador to Turkey has now escalated into a full-scale diplomatic row between the EU and Turkey. The e-mail included correspondence between the ambassador and her superiors in Brussels, Turkish bureaucrats, union leaders, academics and journalists.

The e-mail's contents were leaked to a maverick Turkish weekly, which has already published extracts. Its editor suggests that a state institution leaked the correspondence, the details of which have inflamed Turkish public opinion.

Several groups have now filed complaints with Turkish prosecutors seeking the ambassador's instant expulsion. *The Economist* reported a claim by one ultra-nationalist columnist that the ambassador's life was now at risk.

Encrypted websites vulnerable to security breaches

The possibility of security breaches at supposedly "secure" e-commerce sites – an important issue for all online business activities – came to the fore in a March 12th 2002 report by online newswire *AustralianIT*. The newswire quoted an encryption specialist who claimed that digital keys used in Australia to protect at least 20 per cent of websites can be easily cracked and stolen. They are not good enough, he claimed, to protect customers' online transactions.

The encryption specialist argued that Australian e-commerce businesses are choosing speed over security and do not realise the implications. Another specialist argued that Australia's new federal legislation requires companies to take fair and reasonable steps to protect customers' data. Strong digital keys might, therefore, be required to satisfy the legislation.

For further information: www.australianit.news.com.au

Zero Knowledge unveils P3P compliance tool

On March 5th, Zero Knowledge released "P3P Analyzer", a web-based solution that enables companies to see if their privacy policies comply with the Internet Explorer 6 (IE 6) version of P3P (Platform for Privacy Preferences).

P3P turns businesses privacy statements into machine readable code. It enables consumers, with P3P enabled software built into their IE 6 browser, to automatically see if the websites they visit comply with their privacy preferences.

The P3P analyzer tests companies' privacy policies against the P3P settings on IE6, and demonstrates at what point the policy "breaks". The solution also allows companies to compare their performance with other websites in the same market segment and from across the Web.

According to John Beans, vice president of product marketing for enterprise products, the new solution is an easy way for companies to "analyze and monitor their website's compliance with P3P, benchmark it against other sites, and learn more about the standard." Initially available on a ninety-day free trial, the product is part of the Canadian-based company's strategy to move away from the unprofitable consumer market and tap into the corporate sector.

PGP sale falls through

According to John Geralds of news service *Silicon Valley*, Network Associates (NA), a US-based software vendor, has abandoned plans to sell its PGP (Pretty Good Privacy) subsidiary. PGP, which provides privacy enhancing software, was bought in 1997 from owner Phil Zimmerman. However, consumer privacy products have not fared well, mainly because of the wealth of available products that can be downloaded from the web for free.

Jennifer Keavney, vice president of corporate communications at NA said that despite bids, the offers did not match the value of the products. According to Keavney, the attempted sale was further complicated by the fact that PGP encryption software has been incorporated into other NA security products.

Hackers access data through flashing computer lights

Industrial spies and hackers could be accessing valuable data by monitoring the flashing lights on electronics equipment, according to a *Reuters* news story published on March 11th. Research carried out in the US and Britain showed that data encryption devices and communications equipment, such as modems, emit signals that could allow eavesdroppers to piece together information being sent or received.

Use of optical sensor equipment, plus a plain old telescope, means that highly sensitive data could theoretically be intercepted from up to 1.6 kilometres away. In addition, the light signals can be read even if reflected off walls, emitted through curtains, blinds or frosted glass windows. The solution, according to the researchers, is simple enough: keep equipment away from windows, and put masking tape over any flashing lights.

Employee Data Protection

Sweden proposes law on employee data protection

On March 1st, the Swedish Data Protection Board (Datainspektionen) proposed the introduction of a law on the protection of employees' personal data. Based upon the Personal Data Act, the draft law aims to tighten up on regulations that control companies' treatment of its workers' personal information.

The proposed measures would regulate areas such as the monitoring of workers, medical testing, use of manual data, and the processing of sensitive data.

Datainspektionen says that whilst some large companies and public authorities have guidelines on the personal use of company e-mail, it is, nonetheless, a largely unregulated area. Its draft law, therefore, includes a provision intended to define and limit employers' access to personal information stored in e-mail or other electronic formats. It concedes, however, that "absolute protection" of employees' information is "impossible to guarantee" and that in certain circumstances (such as checking for the security of company information, and suspected criminal behaviour) employers will have rights to access that information.

The draft law also proposes a general rule that will prohibit employers from carrying out unnecessary drugs and genetics testing. However, it suggests tests can be carried out in order to safeguard employee security and ensure that workers have the capacity to carry out their tasks.

Meanwhile, the Swedish government has set up a committee to look into the implementation of the Personal Data Act. The committee has been set up following heavy criticism last year by the Swedish democracy minister, Britta Lejon.

For the full draft of the proposed employment law, see: www.naring.regeringen.se/propositioner_mm/sou/pdf/sou2002_18a.pdf

Hong Kong Commissioner moves to protect employee data rights

On March 8th, the Hong Kong Office for Privacy in Personal Data issued a consultation on the draft Code of Practice on Monitoring and Personal Data Privacy at Work. The Code is to provide practical guidance to those who monitor and record employee activities and behaviour at work.

"To the extent that information contained in monitoring records amount to personal data, they should be collected in a way that is fair in the circumstances, and for a lawful purpose related to a function or activity of the employer," said the Commissioner in a press release.

The 2001 Data Users Survey, conducted by the Commissioner's Office, found that 63.6 per cent of respondent organisations had installed at least one type of employee monitoring device, with one in three installing two or more. The findings also indicated that only 22.1 per cent of organisations surveyed had notified employees of their practices through a written employee monitoring policy. "More significantly," stated the Commissioner's press release, "77.6 per cent of respondent organisations agreed that they would support a Privacy Commissioner's Office initiative to develop a code of practice on employee monitoring."

The Sub-committee on Privacy of the Law Reform Commission of Hong Kong recommended in 1999 that a code of practice be considered for all forms of surveillance in the workplace to provide practical guidance for employers, employees and the general public.

"We recognise," said the Privacy Commissioner, "that employers may wish to undertake employee monitoring for apparent reasons in which a range of justifiable grounds are found. However, as such practices are regarded as quite invasive by employees who are targets of the monitoring, and may be in contravention of the Personal Data (Privacy) Ordinance, there arises a need for practical guidance for employers."

Public and private sector organisations, and members of the general public, are invited to send written comments to the Privacy Commissioner's Office by June 7th.

The consultation paper is available on the Privacy Commissioner's Office website at: www.pco.org.hk
See page 14 for interview with the Commissioner.

UK publishes employee code of practice

The first section of a four-part code of practice on the processing of employee data has been published on the Information Commissioner's website. The 56-page document covers the areas of recruitment and selection, including how to deal with application forms, pre-employment vetting, and securing applicants' personal data. The three remaining sections, covering employment records, monitoring and surveillance, and drug testing, are to be published later in the year.

For the full text of the Code, see: www.dataprotection.gov.uk/dpr/dpdoc.nsf
For analysis on the Code, see the March edition of the PL&B UK newsletter.

Australian unions challenge videotaping of employee drug tests

An Australian mining company that began videotaping workers as they provided urine for drug tests has raised the ire of the Australian Manufacturing Workers Union, reported the Age newspaper on February 11th. According to the report, Mount Isa Mines requires new employees and workers in rehabilitation to be videotaped while providing a urine sample in a small cubicle. A company representative said that the cameras were for surveillance only and that images would not be recorded or reproduced. People who objected to being filmed could instead choose to be directly supervised. The workers' union has called the videotaping an invasion of privacy.

Workers dismissed for complaining online

The New York Times reported on January 21st that failed energy giant, Enron, fired at least two employees in the previous two months for posting information or negative opinions about it on Internet message boards.

The newspaper reported that it was not clear how Enron identified

the employees behind the postings. People who post messages on Yahoo often believe that they cannot be traced if they do not use their real names. But, the *Times* reported, many companies have the technical means to track the online activities of employees who use company computers and servers.

Further information: www.nytimes.com/2002/01/21/business/21WORK.html

Experimental office creates workplace privacy issues

IBM and Steelcase, an office furniture company, have developed "BlueSpace," which they describe as an "interactive and personalised" office of the future. The goal of the BlueSpace project, according to IBM, is to "create a new office environment that integrates the physical workspace with advanced computer, sensor, display, and wireless technologies."

One of the highlights of BlueSpace is a touchscreen allowing users to control aspects of their physical environment to suit their preferences. They include temperature, humidity levels, airflow and lighting. They can also share projects, better communicate with team members, and obtain access to real time news feeds.

A computer display projects information onto any surface – wall, desktop or floor. A "guest" badge worn by an office visitor automatically cloaks confidential information by prompting the display to project a generic image.

A third feature provides the user with on-demand visual and territorial privacy. Colour-coded lighting on top of the office's dividing panels alerts colleagues when an employee is away (blue), busy (red), or accepting visitors (green).

But with the technology comes the inevitable privacy issues. The New York Times warns that privacy issues may loom largest "when you turn off the 'I'm busy' light." It goes on to explain that the BlueSpace prototype automatically alerts those people who have registered a need to see you. They could all descend at once, clamouring to be heard. Moreover, the ID chip makes it easy to trace where you are and where you have been. That may heighten security and teamwork, but it also raises the spectre of Big Brother.

However, the newspaper notes that one banking official who recently examined BlueSpace argued that "the technology could let everyone control you, but not if you set rules and manage the process."

A commercial version of BlueSpace may be available by 2003.

For further information: www.ibm.com/news/us/2002/01/143.html

Ford orders UK workers to cut the smut

In March, the *Guardian* revealed that Ford Motor Company had given its UK employees two weeks to spring clean their systems of any offensive material. An internal e-mail told staff that: "The company reserves the right to conduct random audits of its computer resources." Workers were also warned to avoid sending or forwarding on sexually explicit material, adult jokes, and offensive information relating to religion, disability or ethnic origin.

privacy laws & business online

Our website offers a wealth of information about our services, as well as useful links to other privacy websites. Check the site to see:

❑ How we can help you comply with data protection laws ❑ How to recruit data protection staff
❑ Which privacy conferences and workshops to attend ❑ Which publications you need to keep up to date.

We also bring you editorial and content *listings* of the International and UK newsletters' back issues, indexed by country, subject and company, as well as the opportunity to *subscribe* online. In addition, our pages include *links* to data protection authorities worldwide, other privacy organisations and the European Union.

www.privacylaws.com