INTERNATIONAL newsletter
ISSUE NO 64 SEPTEMBER 2002

Editor & Publisher
Stewart H Dresner
stewart@privacylaws.com

Associate Editor
Eugene Oscapella
eugene@privacylaws.com

News Editor
Alan Pedersen
alan@privacylaws.com

Newsletter Subscriptions
Gill Ehrlich
gill@privacylaws.com

Issue 64 Contributors
María Verónica Pérez Asinari
Lily Taranto
Judith A Sullivan
Dan Cooper
Naomi Assia

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

European Union publishes E-communications Directive

The EU Electronic Communications Privacy Directive officially entered into force on 31st July 2002. The directive has now been published on the European Union's website. For a copy of the text, see the following address:

www.europa.eu.int/eurlex/en/dat/2002/l_201/l_20120020731en00370047.pdf

EU plans harmonised data retention law

EU plans for a harmonised approach to data retention could see Communications Service Providers forced to store records of e-mail, telephone, and Internet traffic for up to two years. Last month, the plans were revealed in a draft framework decision – drawn up by the Belgian government – that was leaked to civil liberties group, Statewatch. According to the document, a "period of a minimum of 12 months and a maximum of 24 months for the *a priori* retention of traffic data is not disproportionate in view of the needs of criminal prosecutions as against the intrusion into privacy that such a retention would entail."

Data retention had been one of the more contentious issues surrounding the EU Electronic Communications Privacy Directive adopted in July of this year. The directive allows member states to draft their own data retention legislation when it is deemed necessary for circumstances such as safeguarding national and public security. However, no specific rules were set out as to the length of time that data could be retained and there was no obligation on the part of individual member states to draft such legislation.

Commenting on the proposal, Tony Bunyan, Editor of Statewatch, said: "The right to privacy in our communications…was a hard-won right which has now been taken away. Under the guise of fighting "terrorism" everyone's communications are to be placed under surveillance."

However, the Danish Presidency of the EU has played down the reports. In a press statement it said: "These rumours are based on fundamental misunderstandings, that could have been avoided…" The Presidency admitted recommending that "binding rules should be established" on a harmonised approach to data retention. However, it stated that the finer details of a proposed law - such as the data to be covered and the length of time allocated for retention - were not discussed.

According to the presidency, the proposal is currently under consideration by a Council of Ministers working group and is not expected to be ready for adoption before November of this year.

For the Statewatch report, see: www.statewatch.org
For the EU Danish Presidency's response: www.eu2002.dk

Public outcry over Japan's national database

Some 4.1 million people have been omitted from a new national database after six local authorities refused to register its citizens. The Basic Residential Register Network System, or Juki Net, was launched on August 1st, despite strong public fears over privacy violations. The database compiles personal details such as name, address, gender and date of birth, onto a central government database.

The Japanese government claims the database will enable it to provide more efficient public services and improve government administration. In addition to storing personal

information, Juki Net will also issue each member of the public with a unique ID number, allowing them access to their records.

However, there has been strong public opinion against the creation of a national database. A survey conducted by news agency *Asahi Shimbun* found that nearly 80 per cent of the public wants the government to put off plans for the national database, with many expressing concern that information could be leaked or abused.

Another survey by *Asahi Shimbun* found that it could be relatively easy for privacy breaches to occur. 20 per cent of local authorities reportedly do not have systems in place to check on access to personal information. High costs have been cited as a reason for not introducing technology that can safeguard information and allow authorities to carry out audit trails on access to data.

See p.20 for report on Japan's efforts to combat unsolicited mobile messaging.

Australia: New South Wales Privacy Guidelines

On July 29th, the New South Wales (NSW) Office of Information Technology issued an Online Privacy and Personal Information Protection Guideline for information technology workers in the public sector.

The guideline seeks to help public agencies develop policies and procedures for the effective management of personal information. The guideline is primarily concerned with the responsibilities of agencies and individuals as set out in the NSW Privacy and Personal Information Protection Act (1998).

The guideline focuses on the need for policies to ensure the effective collection, storage, access, use and disposal of information. It is intended mainly for those with direct responsibility for managing personal and private information.

Canada: Legal challenge to stop police use of surveillance cameras

Canada's federal privacy commissioner, George Radwanski, has launched a legal challenge of video surveillance practices by the Royal Canadian Mounted Police (RCMP) in one British Colombia town. The challenge asserts that the surveillance violates both Canadian constitutional law and international covenants dealing with privacy.

In his most recent annual report, the Commissioner sharply criticised the RCMP for continuously monitoring and recording everyone on a public street (*PL&B Int*, Feb 2002, p.12), calling general video surveillance of public streets and public gathering places by the police or other public authorities "the single greatest threat to the fundamental human right of privacy that our society faces." The RCMP responded by maintaining surveillance, but without continuous recording.

Noting that he had been unable to persuade the RCMP or the Solicitor General of Canada (the minister responsible for the RCMP) to stop the practice, the Commissioner concluded that court action was his only recourse.

The commissioner also sought a legal opinion on this surveillance practice from former Canadian Supreme Court Justice, Gerald La Forest. La Forest concluded that the type of video surveillance employed, with or without continuous recording, violated Canada's Charter of Rights and Freedoms.

Further information: www.privcom.gc.ca/media/nr-c/02_05_b_020621_e.asp

DoubleClick settles privacy case

Online advertising and marketing services provider, DoubleClick, is to pay $450,000 towards the cost of enquiries undertaken by ten US state attorneys general. The 30-month long inquiry focussed on an alleged lack of transparency over the collection of data through DoubleClick's online banner advertising services. DoubleClick clients can use consumer-profiling technologies – such as cookies and web beacons – to target adverts at Internet users.

Commenting on the settlement, New York State Attorney General, Eliot Spitzer, said: "When an online contractor can invisibly track nearly every online consumer, consumers deserve to know the privacy cost of surfing the Web."

In addition to the $450,000 payment to meet the costs of the investigation, DoubleClick agreed to a number of conditions aimed at creating greater transparency. DoubleClick clients using the organisation's tracking technologies will be required to notify consumers through their privacy policies. DoubleClick will also be required to set up a subscription-based notification service, informing customers of any changes to its data collection practices. The New York-based organisation has further indicated that it is developing a "cookie viewer" that will identify the categories that may be used to select and target advertisements to consumers.

And, in what is becoming an increasingly recurrent theme in privacy settlements (see the Microsoft settlement story on p.15), DoubleClick will be subject to three independent compliance checks over the next four years, which will assess its adherence to the settlement terms and its own privacy policy. The results of the checks will be made available to customers through DoubleClick's privacy policy.

DoubleClick said that the settlement does not amount to an admission of any wrongdoing. In a statement, Elizabeth Wang, Senior Vice President & General Counsel for DoubleClick, said: "In order to maintain its position as a leader in online privacy, DoubleClick has worked closely with the Attorneys General to build upon the robust privacy practices it has already implemented."

Full details of the settlement can be found at: www.oag.state.ny.us/press/2002/aug/aug26a_02.html

Fax marketer hit with $2.2 trillion lawsuit

US marketing company Fax.com, and various associates, have been hit with a heavyweight lawsuit for $2.2 trillion after reportedly sending out around three million unsolicited faxes a day. The federal and state class action lawsuit was filed by Redefining Progress, a non-profit public policy organisation headed by Internet entrepreneur Steve Kirsch. Commenting on the lawsuit, Kirsch said in a press statement: "The only way that this practice will stop is if enough people step forward and use the legal system to enforce their rights." Kirsch said that unsolicited faxing is not just an annoyance to consumers, but can also endanger public safety. He referred to a case in which over 1,000 simultaneous faxes were sent to a hospital in Washington.

Redefining Progress is seeking $1,500 per unsolicited fax from Fax.com and its telecoms service provider Cox Communications for a period dating back four years. It is also seeking $500 per fax from each of Fax.com's advertisers.

A press release can be found at: www.junkfax.org/fax/news/fax.comAug22Release.doc

US marketers worried over Mexican privacy bill

The online direct marketing newsletter, *DM News,* reported on July 22nd that a data protection bill may be introduced in the Mexican House of Representatives in the autumn. The report quotes Charles Prescott, vice president of international business development at the US Direct Marketing Association, as saying that the bill reflects a "European philosophy about data protection continuing to travel from country to country...That would kill the [marketing] list business. This is a major problem in Germany, Denmark and Austria."

Among the provisions of the proposed bill are two "opt-in" clauses: the requirement of express consent before a company may collect and store information about an individual, and a prohibition on companies transferring a list of people, or their information, to third parties without prior consent.

Further information: www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=21044

"Trusted Travellers" to speed through US airline security?

The *Washington Post* reported in late June that several airlines have begun working on plans for a passenger identification system that would rely on background checks, fingerprints, iris scans and high-tech IDs to verify individuals' identities and speed up security screening at airports.

The system would work by issuing cards to passengers who are willing to undergo a background check and share biometric information (see *PL&B Int*, June 2002, p. 20 about the problems associated with biometrics as tools to enhance security). This system would reduce the extent of the screening the passengers would undergo at airports.

Ontario: "Valid" but fraudulent "breeder documents" raise security concerns

A persistent weakness in developing identity schemes – whether national IDs or passes allowing individuals onto airport tarmacs – lies in the "breeder documents" used to authenticate the identity of the individual, and which act as a basis for issuing these other documents. Breeder documents typically include birth certificates, driver's licences and passports. Forged or stolen breeder documents permit their holders to "authenticate" their identity fraudulently and pose a major threat to the integrity of identity systems based on these documents (see *PL&B Int,* June 2002, p.24-25).

An Ontario case highlights the dangers of relying on apparently authentic breeder documents. Canada's *National Post* newspaper reported on August 15th that five Ontario Ministry of Transportation workers had been charged in connection with a scheme that sold 25,000 "genuine" Ontario driver's licences. By paying several hundred dollars, individuals could obtain a "genuine" licence containing a false identity. These licences would appear to be valid since their details were entered into the Ministry of Transportation's computers.

The newspaper quotes one police officer: "What a perfect way to start. You obtain a driver's licence. You want to open a bank account, they're going to want to see a valid driver's licence. So you open up an account and bank with them for a little while. Then you decide you want a credit card. So, you obtain credit cards. Then you open a chequing account. You've got cheques, credit cards and a driver's licence that say who you are. Can you imagine the repercussions?"

Further information: www.nationalpost.com/search/site/story.asp?id=78C9418E-1FFF-4E42-8926-C87F5CE3F31D

US government physical security: Missing laptops – and guns

In February this year, *PL&B International* reported on the loss or theft of more than 500 Australian government laptops during 2001. Now it seems that their American government counterparts have done the Australians one better.

In addition to losing hundreds of laptops, the US Federal Bureau of Investigation (FBI) has suffered a rash of missing weapons. A report released in August by the Department of Justice Office of the Inspector General said that the FBI had lost 317 laptop computers between October 1st 1999 and January 31st 2002 – about two per cent of its current inventory of laptops. During that same period, the FBI also reported property losses of 212 functional weapons and 142 inoperable training weapons.

The report could not determine whether the loss of laptop computers compromised sensitive or national security information. However, it did not rule out that possibility, noting

that all FBI laptop computers have access to sensitive information and are authorised for processing classified information up to the "Secret" level. Even the FBI could not identify the security levels of most of the stolen laptops. After completing a physical inventory on March 31st 2002, the FBI reported that the security level for 70 per cent of the lost or stolen laptop computers was "unknown".

The Inspector General's report points to lax security measures as the cause of many losses, and the need, in part, to increase employee understanding of the importance of security.

Some losses resulted from the failure of FBI employees to provide adequate safeguards for property assigned to them, and others from failure to adhere to FBI policies regarding the security of these items. To correct such deficiencies and prevent future losses, the report said the FBI must foster an environment where all employees exercise due care for sensitive assets.

The results of a second audit conducted by the Inspector General – this time, of the US Drug Enforcement Administration (DEA) – reported that 229 of the 6,000-plus laptop computers owned by the DEA in 2001 were unaccounted for. According to the DEA, of all the laptop computers in use, only one was authorised to process classified information.

US Senator Charles Grassley sharply criticised the federal government's practices, saying that it had discovered "a core competency of losing computers."

However, there is hope for those who cannot keep track of their valuables. The *New Scientist* magazine reported on August 15th that researchers at the University of Michigan have developed a system that will automatically encrypt all the data on a lost or stolen laptop once its "master" is out of range. This, said the *New Scientist*, should keep data from falling into the wrong hands.

Further information:
www.usdoj.gov/oig/audit/0227/fullpdf.htm;

No evidence to justify EU directive on workers' data

By Alan Pedersen

A report published towards the end of July, examining workplace privacy laws across the EU, suggests that further study is needed to justify calls for additional EU legislation. Although workers' personal data is already covered under the EU Data Protection Directive (95/46/EC), there have been concerns that disparities among national laws could hinder the free movement of workers (and their personal data) within the EU.

Last year, the Employment and Social Affairs Directorate at the European Commission launched a consultation process with the social partners (see *PL&B Int*, Feb 2002, p.22-25) to assess the need for EU-wide legislation relating specifically to workers' data. However, the new report, which was financed by the Commission, suggests a further directive may not be necessary.

Protection of workers' personal data in the European Union: general issues and sensitive data focuses much of its attention on data relating to areas such as health, criminal convictions, or trade union membership. It concludes that some areas have received "little attention" from member states. "It is felt that some issues on workers' data protection…may deserve additional guidance," states the report. Alcohol and drugs testing is cited as one issue that has generally been neglected. Although some countries have addressed the issue, the report states that they have "not done so in a comprehensive way."

The report highlights a number of different initiatives taken at a national level. The UK has been working on a code of practice, while Finland has adopted a specific law relating to the protection of workers' data. In other countries such as Spain, France and Italy, there are privacy statutes and provisions contained within national labour laws. The report says that disparities between regulatory approaches and the content addressed "may pose potential obstacles to the functioning of the internal market." However, it concludes that there is a lack of evidence to back this suggestion and that "further study may be needed."

The upcoming review of the EU Data Protection Directive may provide further insight into the need for additional legislation. However, the results are unlikely to be published before the second stage of the Commission's consultation, which is expected to begin in the next few months. UNICE (Union of Industrial and Employers' Confederation of Europe), one of the social partners involved in the process, has expressed concern that the Commission appears to be pushing ahead its initiative on workers' data despite the fact that the results of the review are yet to come in. David Coleman, an advisor on information society issues at UNICE, said: "We don't think it is appropriate to have these discussions going on separately."

There are also concerns that responsibility for the Commission's initiative lies in the hands of the Employment and Social Affairs Directorate. The feeling is that that there should be more dialogue with the Internal Market Directorate, which has the expertise and experience from drafting the EU Data Protection Directive. However, one industry observer told *PL&B International*: "I don't think there is a sufficient discussion between the two."

Should it be found that there is a hindrance to the internal market, an EU directive may not necessarily be the only solution. "There is a strong belief among the experts that alternative routes of initiative on [a] European level should be further examined," says the report. It cites solutions such as a European-wide code of practice, or a "set of clarifications" detailing examples of good practice or ways in which businesses can apply the EU Data Protection Directive in the workplace.