INTERNATIONAL newsletter
ISSUE NO 60 JANUARY 2002

Associate Editor
Eugene Oscapella
eugene@privacylaws.com

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

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

Issue 60 Contributors
Rosa J. Barcelo
RA Jens Eckhardt
Eugene Oscapella
and
31 contributors to the
Data Protection Roundup

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

Design by ProCreative +44 (0)20 8429 2400
Printed by Triumph Press +44 (0)20 8951 3883

ISSN 0953-6795

privacy news

Australia: Private Sector Data Protection Legislation in Force

Australia's private sector data protection legislation, the Privacy Amendment (Private Sector) Act 2000, came into force on December 21st 2001 (PL&B Feb 01 p. 10, May 01 p.11, Sep 01 p.6). The Act requires organisations covered by it either to comply with the National Privacy Principles or an approved code that provides protection at least equivalent to that of the National Privacy Principles (p.8). The Act came into force on the intended date, despite reported attempts by some business interests to delay its implementation (PL&B Sep 01 p.8).

EU Commission Finds Canadian Data Protection Adequate

The level of protection granted under Canadian law (p.11) to personal data from the EU is "adequate", according to a formal Decision adopted by the European Commission on December 20th 2001.

Council of Europe Cybercime Treaty Comes Under Fire

When asked about the year's most important developments in law and technology, lawyer Barry Steinhardt of the American Civil Liberties Union had harsh words for the Council of Europe Cybercrime Treaty (PL&B May 01 p. 17). He told the *New York Times* that the signing of the Cybercrime Convention by the US and dozens of other nations would force the signatory nations (ratification by the Senate is necessary in the US) to use draconian means to spy on their own residents. This is so even when the action being "investigated" is perfectly legal in the country that is required to do the spying. Says Steinhardt, "the US, through which most of the world's Internet traffic flows, could be turned into the secret computer police for nations ranging from France to Bulgaria."

Biometrics and Security

The *New York Times* reported on December 17th 2001 that the events of September 11th have led to a surge in requests for biometric products. The security-oriented core of the biometrics industry totalled just under $400 million in 2000, but is now expected to reach almost $2 billion in 2005. One biometrics company spokesman suggested that September 11th could speed up the use of biometrics by three or four years. The newspaper reports further that biometrics companies are cheered by polls showing that Americans would be willing to give up some privacy if that was the price of better security. Still, there was widespread unease among Americans about whether the information obtained from biometrics devices might be abused by government agencies, employers or business.

Among the uses identified in the article for biometric technologies are:

- at border crossings, to speed up the passage of frequent travellers who agree to have their scans on record. Initial programmes are already under way at Heathrow Airport in London and in the Netherlands proving the identities of people carrying credit or identity cards

- to control access to data networks

- to track when and where the records are opened or altered. This will be particularly important in light of major changes to US healthcare regulations.

News continued on page 26