www.privacydataprotection.com

ISSN 1473-3498

Privacy & Data Protection

Volume 6, Issue 6

June 2006

Headlines:

- Veterans claim $26 billion for data breach, p.13
- Patients at risk from data outsourcing, p.14
- Data lost on 1.3 million students, p.15
- Lords demand more data for voting rights, p.16

Inside this issue:

United States agreement on passenger data overturned

The European Union's highest court has ruled that current EU-US passenger data transfer arrangements are unlawful.

The trans-Atlantic agreement, made in 2004 between the US Department of Homeland Security and the EU Commission and Council, compels European airlines to turn over 34 pieces of information about each passenger (Passenger Name Record information)—including name, home addresses and credit card details—within 15 minutes of departure of any commercial aircraft bound for the US from Europe.

Washington maintained that it needed the extensive PNR data for "preventing and combating terrorism and other transnational serious crimes." The 2004 agreement allowed United States authorities to store the data for over 3 years.

On 27th May, the European Court of Justice overturned both the adequacy finding by the European Commission and the Council Decision on PNR data transfers.

The court has given the European Commission until 30th September to find an alternative legal footing for PNR transfers. It is also open for Member States to agree their own bi-lateral arrangements with the United States, although such a move is not favoured by the Article 29 Working Party, which is strongly encouraging an EU-US solution.

Stewart Baker, an assistant secretary of state for the US Department of Homeland Security, said, "I am confident that we will find a solution that will keep the data flowing and the planes flying."

(Continued on page 13)

Commissioner pushes for prison sentence for data crime

Current sentencing levels do not deter perpetrators in the highly lucrative trade of buying and selling personal data, according to the UK Information Commissioner.

Under UK law, the maximum punishment for 'obtaining or disclosing' personal data is a £5,000 fine in the lower criminal courts and an unlimited fine in the higher courts.

In a move that seems to be supported by the government, Richard Thomas, the Information Commissioner, is calling for the law to be changed to allow convicted persons to be sentenced to 2 years imprisonment.

Mr Thomas, in a report laid before Parliament in May, stated that, "all cases in this illegal trade share in common that they involve personal and private information, and that the organisation holding the information has not authorised its disclosure."

Investigations by the Commissioner's Office and the police have uncovered evidence of a widespread and organized undercover market in confidential personal information.

Common types of organisations from which personal data are snatched include telecommunications companies, supermarkets, banks, transport operators, government departments, local authorities, the National Health Service and the police.

The perpetrators include private detectives (who often operate on behalf of

(Continued on page 13)