www.privacydataprotection.com

ISSN 1473-3498

Privacy & Data Protection

Volume 4, Issue 7

July/August 2004

Headlines:

- Record fines for scam texts, p.14
- Sebastian Coe—privacy confusion, p.15
- Iceland DNA project unconstitutional, p.15

Inside this issue:

Employers fear reversal of law as EU investigates UK data laws

Following his defeat in the Court of Appeal in December, Mr Durant has indicated that he will not be giving up—he will be complaining about the UK's data laws to the authorities in Europe.

In *Durant v FSA* (2003) the judges, interpreting the provisions of the Data Protection Act 1998, dramatically restricted the scope of 'subject access requests' by narrowly construing the definitions of 'personal data' and 'relevant filing system.'

In an application filed with the European Commission in late May, Mr Durant alleges that the UK failed to properly implement the EU Data Protection Directive into national law.

Masons, the law firm acting for Mr Durant on a pro bono basis, is not letting their defeat in the Court of Appeal in December stop them. Dr Chris Pounder of Masons said that, "In our view, the Directive's guarantee of the data subject's right of access is seriously undermined by the breadth of judicial discretion assumed by the English Courts in relation to section 7(9) of the Data Protection Act 1998.

"We are also of the view that there are arguments that the implementation of the Directive's provisions in respect of the meaning of personal data, can also be challenged."

Employers bear the brunt of subject access requests and have complained to the government about excessive costs of compliance that the law imposes (see *Privacy & Data Protection*, Volume 3, Issue 3, page 3 for an analysis of the Lord Chancellor's 2003 review of the subject access right).

Although employers and others had given a cautious cheer to the ruling in *Durant*, this new action threatens the more restrictive stance that they have been advised to take since the case.

(Continued on page 14)

EU agrees PNR transfers to US

The European Union has finally approved a scheme for the transfer of air passenger details from European countries to the United States.

The US Bureau of Customs and Border Protection ('CBP') has insisted, since soon after 9/11, on being given electronic access to the data, as part of the 'war on terror.' The EU has resisted the transfer of Passenger Name Records ('PNR') data on the basis that such transfer breaches EU data protection laws.

The EU Data Protection Directive prevents the transfer of personal data outside of Europe without there being 'adequate protection' for the privacy of individuals. The new scheme apparently meets these requirements.

PNR data are held in the electronic reservation systems of airlines and consist of 34 categories of information concerning passengers flying from Europe into the United States—PNR data include name, address, email address, frequent flier information, travel status, seat number and bag tag numbers.

Under the scheme, the US will be permitted to use PNR data for the purposes of combating terrorism and serious crime. It will also be allowed to transfer the data to other governments for similar purposes.

Of the 25 Member States of the EU, 21 countries voted for the measure and 4 countries voted against it.

It is known that the US has

(Continued on page 14)