www.pdpjournal.com

ISSN 1473-3498

Privacy & Data Protection

Volume 8, Issue 1

October / November 2007

Headlines:

- German Commissioner criticises Google, p.17
- Eircom security flaw, p.18
- Irish private sector guidelines p.19
- Loan applications sold to competitors, p.19

Inside this issue:

UK — newly awarded access to phone records too wide?

A substantial extension of surveillance powers has recently come into force in the UK. The new powers give police, government officials and local councils unprecedented access to telephone records and force telecommunications companies to retain information about all landline and mobile phone calls made by members of the public for one year.

The move was approved by the UK Parliament in July under the Regulation of Investigatory Powers Act 2000, with the powers coming into force at the end of September. More than 650 public bodies and quangos are the potential recipients of the data.

Those awarded with the new powers include tax authorities, 475 local councils, NHS Trusts, ambulance and fire services, and government departments including the Food Standards Agency, the Department of Health, the Immigration Service, the Department for the Environment and the Charity Commission.

To access the phone records, officials must first get approval from a senior staff member, but levels of access to the systems are also dependant on the type of authority requesting the information. For example, police and intelligence services will be able to see more detailed information than local authorities, whereas NHS Trusts and ambulance and fire services can only request access in rare life-saving cases.

Home Secretary, Jacqui Smith, signed the statutory instrument made under the European Communities Act 1972, on 26th July. It attracted little notice at the time because it was introduced into UK law by a statutory instrument, rather than by a new Act of Parliament. The move brings into UK law a European directive, the Data Retention Directive, aimed at "the investigation, detection and prosecution of serious crime."

(Continued on page 17)

Europe to adopt security breach notification requirements

A requirement on companies to notify security breaches involving personal data will become compulsory in European law, according to the European Data Protection Supervisor ('EDPS').

Speaking at the 6th Annual Data Protection Compliance Conference in London on 11th October, Peter Hustinx, the EDPS, said that the drafting of the new law will require considerable thought. "One issue to be resolved is to whom the security breach should be notified," he said.

There are three main groups of interested parties to whom notification of a security breach can be directed: clients (or customers), the relevant data protection (or other) authorities and the public in general. According to Hustinx, the notification "needs to be to the public because it needs to be visible—if its not visible, its not going to work."

The possible instigation of a notification requirement in Europe has been on the agenda since California enacted security notification law. There is a growing feeling that the public finds it 'unfair' that organisations in the public and private sectors should effectively be allowed to hide the fact that a security breach has occurred which affects their personal information.

(Continued on page 17)