www.pdpjournals.com

ISSN 1473-3498

Privacy & Data Protection

Volume 9, Issue 5

April/May 2009

Headlines:

- Fools rush in to hiding behind DPA, says ICO, p.17
- 19,000 UK credit card details accessible, p.18
- EU: 'security capabilities vary vastly', p.19
- Stronger penalties for peeping toms, p.20

Inside this issue:

Editorial 2

BSI —a standard approach to preventing security breaches? 3

A fair processing notice by any other name … 6

US pre-trial discovery — reconciled with European data protection law? 8

Dirty work — criminal aspects of bin trawling 12

Spam Asia — Part II 14

News & Views 17

Internet data now stored for 12 months

Internet service providers are now storing the web and email traffic details of UK citizens for 12 months in implementation of the Data Retention (EC Directive) Regulations 2009.

A Home Office spokesperson said: *"It is the government's priority to protect public safety and national security. That is why we are completing the implementation of this directive, which will bring the UK in line with our European counterparts.*

"Communications data is the where and when of the communication and plays a vital part in a wide range of criminal investigations, and prevention of terrorists attacks as well as contributing to public safety more generally...

"Access to communications data is governed by Regulation of Investigatory Powers Act 2000 (RIPA) which ensures that effective safeguards are in place and that the data can only be accessed when it is necessary and proportionate to do so".

The Data Retention Directive was passed in 2006. The first phase of the legislation required telephone companies to store records of where and when calls were made. The second phase deals with the retention of internet traffic data.

The EU legislation allows countries to choose a retention period of between six and 24 months. The UK has chosen a period of 12 months.

The new legislation means that internet service providers must retain data on what communications were made, from which internet protocol (IP) address or phone number, what the destination of that communication was, and its duration.

(Continued on page 17)

EU governing bodies urged to introduce surveillance register

The European Parliament has adopted a resolution which recommends that EU governments take proactive measures to strengthen security and fundamental freedoms of on the internet.

Under the resolution, the EU governments are urged to create a list of all organisations that track internet use, and to produce annual reports on internet surveillance.

The Members of the European Parliament recommend 'full and safe access to internet for all', 'a strong commitment to tackling cybercrime', constant attention to fundamental freedoms (of individuals), and a renewed commitment to an on-going 'internet bill of rights'.

Of the third proposal, the European Parliament said that governments should *"recognise the danger of certain forms of internet surveillance and control aimed also at tracking every 'digital' step of an individual, with the aim of providing a profile of the user and of assigning 'scores'."*

"They should 'make' clear the fact that such techniques should always be assessed in terms of their necessity and their proportionality in the light of the objectives they

(Continued on page 17)