



# Privacy & Data Protection

Volume 10, Issue 5

April/May 2010

## Headlines:

- ICO publishes three year plan, p.17
- Europe investigates 'tagging', p.18
- EDPS wants privacy designed into DP law, p.19
- And the award for best data protection goes to..., p.20

## Inside this issue:

Editorial	2
Working Party confirms 'controller' and 'processor' distinction	3
Data protection: back to basics — Part 5	6
Data subjects rights — are they inadequate?	8
Changes to German data protection law	10
Where fines might hit the hardest	13
News & Views	17

## NHS breaching citizens' human rights over levels of access

The potential access to access confidential patient records at UK hospitals is breaking Human Rights laws, according to persuasive new research.

UK campaign group, Big Brother Watch, surveyed 151 NHS Trusts (more were asked for responses, but 28% failed to respond to requests). Amongst its key findings, non-medical staff — including receptionists, housekeepers and porters — could access confidential patient records if they wanted, and an average of 723 of such staff (not involved in direct patient

care) per NHS Trust had access to medical records.

The research concluded that the NHS Trusts are in direct contravention of the European Court of Human Rights' ruling in 2008 in *I v. Finland* which established a legal duty to restrict medical records only to those directly involved in personal care.

David Smith, Deputy Information Commissioner, told *Privacy & Data Protection* that "robust criteria" need to be applied to ensure the numbers of people who have access to

medical records are kept to a minimum. He said "patients' records should only be accessed by those who need them to do their job and all staff must be obliged to observe strict confidentiality rules. Not all staff need the same level of access to patients' records and there must be effective solutions available to vary the level of access to ensure it is commensurate with a job role."

The ICO is now studying the report and "will not hesitate to make our own enquiries with the NHS if further action is required."

## ICO urges proportionality over police use of internet cafes

The Information Commissioner's Office has warned the police to approach their latest anti-terrorism initiative with caution to ensure that it does not contravene data protection legislation.

The police will use internet café surveillance as part of a trial scheme being piloted in London whereby owners agree to monitor what customers are looking at, and report any suspect activity to police. The surveillance

has already started in cafes in Camden.

It is being justified on the basis of evidence suggesting that several people convicted of terrorism offences have visited internet cafes while plotting their crimes.

If it is successful, the Metropolitan Police hopes other police forces, as well as universities, will adopt the measures.

A spokesperson for the Information Commissioner's Office told *Privacy & Data Protection* that it recognises the value that information about people's communications can have for the prevention and detection of crime, and the prosecution of offenders.

The ICO said "however, we would urge a proportionate approach with proper safeguards to ensure that this form of

*(Continued on page 17)*