



Privacy & Data Protection

Volume 9, Issue 6

June 2009

Headlines:

- BCS launches data protection “equivalent of Highway code,” p.17
- EU sues Sweden, p.18
- Germany to get Street View despite privacy complaints, p.19
- Resignation of rail chief after repeated snooping, p.20

Inside this issue:

Editorial	2
Secondary uses of personal data in the NHS — Part 1	3
Surveillance at the workplace — how to avoid the pitfalls	8
Richard Thomas — the expansive years	11
Privacy and matrimonial ‘self-help’	12
News & Views	17

Drug and prostitute habits are “routine” at the MoD

The personal data of senior RAF staff, including their histories of drug abuse and sexual preferences, went missing as part of a data loss incident last September that was described by the UK Ministry of Defence at the time as just a loss of “routine vetting information.”

When three unencrypted computer hard drives containing 500 files went missing, the MoD said that only bank details and home addresses were contained in the files. However, the results of a recent Freedom of Information Act request have revealed

that what in fact went missing was information that “relates to those cases that have been referred to RAF because the individuals have serious vulnerabilities that affect their suitability to obtain/retain a security clearance.” The facts about the incident were detailed on an internal MoD memo recently published by the *Guardian* newspaper. The 500 staff affected, who face potential exposure to blackmail over their vices, have apparently been contacted.

In addition to details of extra marital affairs and

drug habits, the missing data included criminal convictions, investigations, debt history and medical conditions. All in all, “an excellent target list for foreign intelligence services, investigative journalists and blackmailers,” according to the memo.

A MoD spokesman has said there is “no evidence to suggest the information held on the hard drive has been targeted by criminals or hostiles.” News of the loss was placed prominently on the MoD and RAF websites, and an emergency helpline has been established.

New ICO Code on Privacy Notices

The Information Commissioner’s Office (‘ICO’) is launching a new and first of its kind Code of Practice on Privacy Notices.

The Code has taken the ICO over 12 months to produce. Speaking at the 2nd Annual Data Protection in the Public Sector Conference, Ian Bourne, Head of Data Protection Projects at the ICO, revealed that the ICO spent several weeks trawling through organisations’ “poor and unintelligible” Privacy

Notices, even before the public consultation opened.

Mr Bourne said that one of the major existing problems is the difficulty organisations experience in distinguishing between the requirements for ‘transparency’ and to obtain individuals’ consent prior to data processing, in the Data Protection Act 1998 (‘DPA’). Apparently, the new section clarifying what the DPA says will assist organisations in this area.

The consultation process revealed that one of the main points of contention from the private sector was the ICO’s stance on opt-in and opt-out provisions. (For instance, all of the examples of ‘good practice’ in the draft Code included the provision of an opt-in for marketing, as opposed to consent via an opt-out process).

Mr Bourne said that such clauses in fact “act as a red herring in many cases,” and that organisa-

(Continued on page 17)