www.pdpjournals.com

ISSN 1473-3498

Privacy & Data Protection

Volume 9, Issue 8

September 2009

Headlines:

- Smartphone applications track users' locations, p.17
- Google to address Swiss concerns, p.18
- IRS brings in the heavies for tax scour, p.19
- Facebook accepts Canadian privacy recommendations, p.20

Inside this issue:

ICO calls for organisations to encrypt all mobile devices

The UK's Data Protection Authority, the Information Commissioner's Office, has called for all organisations to ensure that they encrypt their mobile devices.

The instruction has come as part of the ICO's recent enforcement action against transport company UPS. An unencrypted password-protected laptop was stolen from one of UPS's employees during a business trip abroad in October 2008. The laptop, never recovered, contained the personal data of approximately 9,150 UK based UPS employees.

The lost information included employees' names, addresses, dates of birth, National Insurance numbers, and salary and bank details. The UK employees were notified by UPS shortly after the theft, and precautionary measures were organised for them.

UPS has signed a formal undertaking with the ICO, agreeing to a number of measures, including ensuring that "appropriate data security programmes and procedures regarding removable media, including the use of encryption where appropriate, are put in place within six months."

Assistant Information Commissioner, Mick Gorrill, said "I urge all organisations to restrict the amount of personal information that is taken off secure sites. I am pleased that UPS has encrypted its laptops and smartphones, and I urge other organisations to follow suit."

UPS has also agreed to train all relevant staff on security and data protection procedures.

According to Peter Carey, author of '*Data Protection — a practical guide to UK and EU law*', "The UPS undertaking is the latest in

(Continued on page 17)

Information Commissioner: plans to collect communications data go too far

The Information Commissioner has expressed his concern over the extent of the collection of communications data proposed in the UK government's Interception Modernisation Programme.

Communications Service Providers are currently required to retain data that can be examined by authorities for a period of 12 months (under the Data Retention (EC Directive) Regulations 2009).

The UK government is consulting on plans to force communications companies to collect and process further information on internet activity.

The Commissioner has responded to the plans saying that, though he recognises the value that communications data has for the prevention and detection of crime and the prosecution of offenders, that that is not in itself "a sufficient justification for mandating the collection of all possible communications data on all subscribers by all communication service providers."

One of the Commissioner's reservations is that just because certain communications data have proved useful in the past, does not necessarily mean that the collection of the communications data of the entire

(Continued on page 17)