www.pdpjournals.com

ISSN 1473-3498

Privacy & Data Protection

Volume 8, Issue 8

September 2008

Headlines:

- Draft 2008 Electronic Communications Regulations, p.17
- Students subject to scanners, p.18
- Fingerprinting of passengers inevitable, p.18
- Unsecured data stick puts *Gastronuts* kids at risk, p.19

Inside this issue:

Searching questions as prison data makes a break

A contractor working for the Home Office has lost a memory stick containing the personal data of all 84,000 prisoners in England and Wales. The stick also contained the unencrypted information from an electronic system used for monitoring offenders through the criminal justice system, including data on 10,000 persistent offenders.

The loss comes just weeks after the publication (in the Department's Resource Accounts) of a similar data loss at the Home Office. That incident occurred in back in March, when an external contractor sent two password protected discs to the UK Border Agency by normal post instead of special delivery. The Home Office responded by committing to work closely with the contractor concerned to ensure compliance; introducing an encryption service for data sent by post; and instructing employees to use a recorded delivery service. The measures have proved to be inadequate in preventing similar incidents.

Chris Potter, Partner at PricewaterhouseCoopers LLP, said the problem is to do with the amount of 'controls' employed:

"Most drastic data security breaches involve a breakdown in multiple controls, any one of which would have prevented the breach occurring. It's easy to focus on technology after an event, but for effective control they need a combination of people, process and technology. Organisations need to address not only the specific controls that might address this breach but also the general conditions that make breaches more common.

"Business[es] and organisations need to be wary of specific weaknesses in

(Continued on page 17)

Bidder's hard drive for bargain on data

A server containing the personal data of millions of American Express, Royal Bank of Scotland and NatWest customers on its hard drive has been sold on eBay. The £35 purchase contained sensitive information including account numbers, passwords, mobile telephone numbers, and signatures, all of which could be used to impersonate others.

The loss came about when the server was inappropriately sold by an ex employee of archiving firm Graphic Data. Graphic Data has said in a statement that it had not planned to dispose of the server, and was investigating how it had appeared on eBay:

"The IT equipment that appeared on eBay was not planned to be disposed [of] by the company and investigations are still ongoing to find out how this equipment was removed from one of Graphic Data's secure locations."

The former employee reportedly sold the computer server without wiping the internal hard drive. Ebay has confirmed it would not allow the open selling of bank details on its site.

The potential breach was notified when eBay customer and purchaser of the server, IT Manager from Oxford Andrew Chapman, located the information. Chapman said the information was "easy to find if you know something about computers." Chapman was also very vocal about his faith in the ability of the ICO to deal with the matter, telling the *Oxford Mail* that the ICO did not

(Continued on page 17)