www.pdpjournal.com

ISSN 1473-3498

Privacy & Data Protection

Volume 7, Issue 8

September 2007

Headlines:

- Microsoft takes lead in online privacy, p. 17
- £14bn red tape cuts unrealistic, p.17
- ID scanning probe approved, p.18
- No breach of confidence for JK Rowling, p.19

Inside this issue:

Trojan breach at Monster.com leads to phishing emails

The job recruitment website Monster.com has suffered a large scale data breach, when stolen log on details were used to access the site.

A Trojan virus accessed Monster.com with the log on details and searched for all available resumes — potentially lifting the name, email address, home address and phone numbers of its victims.

The virus then successfully posted the stolen information onto a remote server controlled by the attacker, now identified as two server computers at a web-hosting company in Ukraine.

The security breach has affected up to 1.6 million files on the server, mostly based in the US.

Patrick W. Manzo, Vice President of compliance and fraud prevention at Monster.com said "to the best of our knowledge, this is not a hack of Monster's security, rather, legitimate customer credentials are being used to log in to the database." He added, "there have been reports of this as an issue of identify theft."

Symantec, the security firm that first discovered the breach, reported it had seen reports of phishing emails sent out to Monster.com users which were "very realistic, containing personal information of the victims." These emails were a secondary attack on the Monster.com users, and were activated by the data collected by the initial Trojan virus breach.

The emails advise members to download a job seeker tool from Monster.com, but in reality the download encrypts files on the affected computer — leaving a text file demanding the victim pay the attackers in order to recover the data.

Monster.com has been working to halt the collection of customers' information, and said "When we see an unusual amount of downloading of

(Continued on page 17)

UK launches CCTV code

The Information Commissioner's Office, the UK data protection regulator, has launched a consultation on its new draft CCTV code of practice, which sets out good practice advice for those involved in operating CCTV cameras.

The draft code is aimed at organisations which routinely capture images of individuals on their CCTV equipment and will help them to comply with the Data Protection Act.

One interesting development is that the new draft code states that CCTV must not be used to record conversations between members of the public, as this is "highly intrusive and unlikely to be justified." If a CCTV system is equipped with a sound recording facility, it should always be turned off or disabled.

The Information Commissioner, Richard Thomas, has previously warned that the UK is becoming a "surveillance society" without sufficient debate about what that involves. The UK has more CCTV cameras per head of population than any other country in the world — 4.2 million cameras represents one for every 16 people.

Jonathan Bamford, Assistant Commissioner at the

(Continued on page 17)