www.pdpjournals.com

ISSN 1473-3498

Privacy & Data Protection

Volume 9, Issue 3

January/February 2009

Headlines:

- New IC says role is at heart of debates, p.17
- New NAI Principles just don't cut it?, p.18
- Coming to a cab driver near you?, p.19
- College kids enlisted in data gathering, p.20

Inside this issue:

Police hack into homes

The UK's Home Office has adopted a new plan to allow police across Britain to "remote search" personal computers routinely and without a warrant.

It follows the decision taken by the Council of Ministers for the European Union in November 2008 to "fight against cyber crime." According to a press release issued at that time, "the strategy proposes a series of operational measures, such as cyber patrols, joint investigation teams and remote searches to become part of the fight against cybercrime in the next five years."

The new plans will allow police or MI5 officers based hundreds of miles away to examine a hard drive at someone's home, office or hotel room, covertly.

The intrusive surveillance powers may be granted if a senior officer says he believes that it is proportionate and necessary to prevent or detect serious crime — which is defined as any offence attracting a jail sentence of more than three years.

The strategy would also allow German, French, and other police forces in the EU to request that British officers hack into someone's UK based computer, and hand over any information gleaned. Material gathered might include the content of emails, web-browsing habits, and instant messaging.

Remote searches, though very rarely deployed, have been possible since 1994 via an amendment to the Computer Misuse Act 1990. Under that Act, authorities could break into a suspect's home or office and insert a "key-logging" device into an individual's computer. This would collect and, if necessary, transmit details of all the suspect's keystrokes.

This type of surveillance is closely regulated under the Regulation of

(Continued on page 17)

Private firms to control data "hellhouse"

The UK government is to publish a consultation paper containing the key option that the private sector manage and run a communications database that will keep track of individuals' telephone calls, emails, texts and internet use.

Until now most communications traffic data has been held by phone companies and internet service providers for billing purposes.

The Home Secretary, Jackie Smith, postponed the introduction of legislation to set up the super database in October 2008, opting to publish a consultation paper in the new year setting out the proposal and the safeguards needed to protect civil liberties.

It is likely that the proposal paper would state that any cabinet decision to place the management of the super database of all UK communications traffic into private hands would be accompanied by stricter legal safeguards.

The Home Secretary has emphasised that communications data, which gives the police the identity and location of the caller (texter or web surfer), but not the content, has been used as important evidence in 95% of serious crime cases, in addition to almost all security service operations since 2004 including the Soham and 21/7 bombing cases.

Former Director of Public Prosecutions, Sir Ken Macdonald has warned it

(Continued on page 17)