



**People for Proper Policing in North Wales**

## **Police set to step up hacking of home PCs**

David Leppard The Sunday Times January 4, 2009

**THE Home Office has quietly adopted a new plan to allow police across Britain routinely to hack into people's personal computers without a warrant.**

The move, which follows a decision by the European Union's council of ministers in Brussels, has angered civil liberties groups and opposition MPs. They described it as a sinister extension of the surveillance state which drives "a coach and horses" through privacy laws.

The hacking is known as "**remote searching**". It allows police or MI5 officers who may be hundreds of miles away to examine covertly the hard drive of someone's PC at his home, office or hotel room. Material gathered in this way includes the content of all e-mails, web-browsing habits and instant messaging.

**Under the Brussels edict, police across the EU have been given the green light to expand the implementation of a rarely used power involving warrantless intrusive surveillance of private property.** The strategy will allow French, German and other EU forces to ask British officers to hack into someone's UK computer and pass over any material gleaned.

A remote search can be granted if **a senior officer says he "believes" that it is "proportionate" and necessary to prevent or detect serious crime** — defined as any offence attracting a jail sentence of more than three years.

However, **opposition MPs and civil liberties groups** say that the broadening of such intrusive surveillance powers should be regulated by a new act of parliament and court warrants.

They point out that in contrast to the legal safeguards for searching a suspect's home, police undertaking a remote search do not need to apply to a magistrates' court for a warrant.

**Shami Chakrabarti, director of Liberty**, the human rights group, said she would challenge the legal basis of the move. *"These are very intrusive powers – as intrusive as someone busting down your door and coming into your home,"* she said. *"The public will want this to be controlled by new legislation and judicial authorisation. Without those safeguards it's a devastating blow to any notion of personal privacy."*

She said the move had parallels with the warrantless police search of the House of Commons office of **Damian Green, the Tory MP**: *"It's like giving police the power to do a Damian Green every day but to do it without anyone even knowing you were doing it."*

**Richard Clayton, a researcher at Cambridge University's computer laboratory**, said that remote searches had been possible since 1994, although they were very rare. He said the 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. *"It's just like putting a secret camera in someone's living room,"* he said.

**Police might also send an e-mail to a suspect's computer. The message would include an attachment that contained a virus or "malware". If the attachment was opened, the remote search facility would be covertly activated. Alternatively, police could park outside a suspect's home and hack into his or her hard drive using the wireless network.**

Police say that such methods are necessary to investigate suspects who use cyberspace to carry out crimes. These include paedophiles, internet fraudsters, identity thieves and terrorists.

**The Association of Chief Police Officers (ACPO)** said such intrusive surveillance was closely regulated under the Regulation of Investigatory Powers Act. A spokesman said police were already carrying out a small number of these operations which were among **194 clandestine searches last year of people's homes, offices and hotel bedrooms.**

*"To be a **valid authorisation**, the officer giving it must believe that when it is given it is necessary to prevent or detect serious crime and [the] action is proportionate to what it seeks to achieve,"* **ACPO** said.

**Dominic Grieve, the shadow home secretary**, agreed that the development may benefit law enforcement. But he added: *"The exercise of such intrusive powers raises serious privacy issues. The government must explain how they would work in practice and what safeguards will be in place to prevent abuse."*

The Home Office said it was working with other EU states to develop details of the proposals.

**The PPP comments ... before Brunstrom joined NWPF we was labeled Disingenuous by a judge. He had misused the police phone tapping powers and jeopardized a criminal court case. He and NWPF have since been guilty of many other abuses including those in the Peter Bolton witch/mole hunt and many corrupt speed camera prosecutions including 6500 scanned signatures. We reluctantly conclude that if we grant them the powers the abuse/misuse has followed. ACPO, quoted above appear to turn a blind eye to abuses of their own codes of practice and conduct. Ian Blair and Meredith Hughes being just two other examples. Note they are developing details of the proposals after 194 such searches last year.**