Britain: New cybercrime police force threatens civil liberties

Mike Ingram
20 April 2001

Labour Home Secretary Jack Straw launched a specialist police unit designed to tackle computer-based crime on Wednesday.

Speaking to the BBC Straw said, “Our overall approach is that if something is criminal offline it is also criminal online. But we have to ensure that police investigatory techniques keep up with changes in technology.”

Responding to widespread criticism, the unit's Detective Chief Superintendent Len Hynds told BBC News, “We have no inclination, nor the desire, nor the ability to trawl peoples e-mails. We will be targeting those people who use the Internet to commit fraud, paedophilia and other offences.”

But under the pretext of combating crime, the Labour government has granted unprecedented powers to the state forces to intrude into the private lives of every individual in Britain and anyone from overseas who corresponds with the UK electronically.

The National Technical Assistance Centre (NTAC) will be based at a £25 million unit and will draw its staff from individual police forces, Customs, the National Crime Squad (NCS) and the National Criminal Intelligence Service (NCIS). Plans to set up the unit were first announced last year as part of the Regulation of Investigatory Powers (RIP) bill.

The RIP designates Internet Service Providers (ISPs) as "public telecommunications systems" and requires them to give access to detailed information about Internet traffic upon the demand of the Home Secretary, a judge or a senior police officer.

The job of the new force is to sift through the information gathered through so-called “black-box” devices that ISPs are to be compelled to install, allowing information to be filtered to the new centre.

NTAC will have permanent links to Britain's Internet connection companies, making it easy to intercept email, chat sessions or any other data passing over the networks of these companies. To thwart the use of encryption software to prevent monitoring, RIP gives the police the power to demand the codes to read all encrypted messages. This includes the codes used by business to protect credit card numbers in electronic commerce transactions.

In what RIP opponents have correctly termed a violation of the presumption of innocence, failure to comply with a decryption notice will be a criminal office unless the person can prove they did not have the ability to decrypt the message for any reason, such as losing the password.

Concerns raised by civil liberty campaigners at the time of RIP's introduction have now been voiced by MPs. A report written by members of the Commons Intelligence and Security Committee (ISC) expressed fears that the new force and the RIP legislation could come into conflict with Britain's adoption of human rights legislation.

The report also criticises the Investigatory Powers Tribunal (IPT), created by the government to allay fears of widespread breaches of Internet users' privacy rights. The IPT was supposed to act as a court of appeal for anyone who believes that investigating officers have unlawfully intercepted their communication when collecting evidence. The ICS express concern that the IPT is ill equipped to do its job.

During a debate on the report, ISC member Alan Beith described as “ludicrous” the poor staffing levels of the Tribunal. “The several bodies involved are dependent on a tiny support structure which is quite incapable of carrying out the job. We are not providing a safeguard that should be there,” he said.

The criticisms of the ISC will do nothing to curtail

the threat to democratic rights posed by the new force. The obvious question remains how anyone will know if his or her rights have been violated in the first place.