British intelligence services seek wide powers to spy on phone calls and Internet usage

Mike Ingram
6 December 2000

According to a December 3 article in the *Observer* newspaper, "Britain's intelligence services are seeking powers to seize all records of telephone calls, emails and Internet connections made by every person living in this country."

The newspaper claims to have received a document circulated to Home Office officials revealing that MI5, MI6 and the police are demanding new legislation to keep a record of every phone call made in the country for as long as seven years.

Secret moves are underway to build a government-run "data warehouse, a super computer that will hold the information," the newspaper claims.

The document says that new laws are needed to allow the intelligence services, Customs and Excise and the police to access telephone and computer records of every member of the public. According to the *Observer*, the Home Office has admitted, "it was giving the plans serious consideration." The document suggests that the Home Office is sympathetic to the new powers, which it says would be used to tackle "the growing problems of cybercrime, the use of computers by paedophiles to run child pornography rings, as well as terrorism and international drug trafficking."

Civil liberties campaigner John Wadham, director of Liberty, said, "The security services and the police have a voracious appetite for collecting up information about our private lives, but this is an extraordinary idea.

"This would violate the principles of the Data Protection Act and the Human Rights Act and the government should reject this idea now. If it goes ahead we will challenge this in the courts in this country and the European Court of Human Rights."

The document admits that the new legislation could clash with the Human Rights Act, which assures certain rights to privacy, European Union law and Britain's Data Protection Act protecting the public against official intrusion into private lives. But this would not be the first legislation to do so.

In October this year, British companies were given the right to spy on their employees' email and telephone calls. Earlier, the Regulation of Investigatory Powers Bill (RIP) was introduced, which among other things enforces police access to people's private keys, electronic code that allows the decryption of emails. The RIP bill also requires Internet Service Providers to install "black box" devices, allowing access by the security forces to email messages hosted on an ISP's computers. The device can transfer data over secure channels to a new Government Technical Assistance Centre, which is to be built at a cost of billions of pounds.

The document revealed by the *Observer* appears to go much further. It would allow the security services to monitor every telephone call made or received by a member of the British public, as well as all emails sent and received. It would also record every web page that an Internet user viewed.

Roger Gaspar, the document's author, is deputy director-general of the National Criminal Intelligence Service—the Government agency that oversees criminal intelligence. Gaspar says it was written on behalf of Acpo (Association of Chief Police Officers), Customs and Excise, MI5 and MI6, and the GCHQ government spy centre at Cheltenham.

Arguing that telephone companies should be ordered to retain all records of calls and Internet access, Gaspar writes: "In the interests of verifying the accuracy of data specifically provided for either intelligence or evidential purposes, CSPs [communication service providers such as telephone or internet companies] should be under an obligation to retain the original data supplied for a period of seven years or for as long as the prosecuting authority directs." He adds, "We believe that the Home Office already accepts that such activity is unquestionably

© World Socialist Web Site

lawful, necessary and proportional, as well as being vital in the interests of justice."

Speaking on BBC Radio 5 Live, Home Office Minister Paul Boateng said the government would strive "to get the balance right" between the demands of industry and the demands of law enforcement. This was a reference to the growing concerns of business that the ever-tighter restrictions placed upon communications, will hamper Britain's global competitiveness in the sphere of e-commerce.

In addition to the invocations of paedophilia, child pornography and terrorism in general, the Tuesday December 5 *Guardian* reported that Gaspar specifically cites the Omagh bombing in Northern Ireland, for which no one has yet been convicted, as a justification for the introduction of the new measures. Individuals suspected of carrying out the bombing, which killed 29 people, have been named in the press, but none have been charged.

On this basis Gaspar argues: "The only evidence currently available to link suspects is that provided by data from the use of their mobile phones. This places them within the proximity of the incident."

He adds that, "Recent advances in location-based customer services have reached the stage where more precise data can now pinpoint the whereabouts of the user of a mobile phone at a specific time. In the absence of any other evidence... communications data will be the only means of securing a prosecution. Deletion of data would seriously damage the ability of the agencies to reactively investigate the acts of terrorism."

Under the guise of a "fight against terrorism" the British security forces are demanding legislation that will make further inroads into basic democratic rights. The secret proposal, like other legislation before it, is not aimed at a criminal or terrorist element, but at the population as a whole. Under conditions of unprecedented social polarisation, the security services are demanding the unhindered ability to track every citizen's movements and communications.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site