British government accessing telephone records

Richard Tyler
18 October 2007

At the beginning of October, the Labour government "activated" part three of the Regulation of Investigatory Powers Act 2000 (RIPA) granting various branches of the state wide powers to access telephone records without recourse to a judge.

According to some reports, up to 800 state bodies and agencies can now seek access to telephone records, including all of Britain's local authorities and even such quasi-non-governmental organisations as the Scottish Ambulance Service Board or the Food Standards Agency.

Security and Counter-terrorism Minister Tony McNulty told BBC Radio 4 that the data could provide three levels of information, with the simplest being about the phone's owner. The second level of data is not merely about the subscriber, "but also the calls made by that phone.

"And the third level, which is purely for the security forces, police, etc., is not just the subscriber information and the calls made, but also the calls coming in and location data—where the calls are made from."

Since telecom operators retain geographic data about the "cells" over which calls are routed, these provide sufficient information to locate a mobile phone. In urban areas, where the cell transmitters are very densely sited, this enables a phone's position to be calculated to within a few feet.

Further powers include demanding encryption keys that may have been used to encrypt data and emails be handed over, with failure to comply attracting a possible prison sentence of from two to five years.

Under section 49 of RIPA, the police can serve a notice requiring encrypted data to be "put into an intelligible form"—i.e., decrypted. It can force people to hand over their encryption keys, which will then be held by the National Technical Assistance Centre (NTAC). According to the Home Office, this is a "twenty-four hour centre operated on behalf of all the law enforcement, security and intelligence agencies, providing a central facility for the complex processing needed to derive intelligible material from lawfully intercepted computer-to-computer communications and from lawfully seized computer data that are increasingly encrypted."

The government has sought to justify this extension of state powers mainly by citing the "fight against terrorism," but it has also admitted that the use of encryption has grown more rapidly than it had anticipated, and that this is also a reason why it has now "activated" the powers already contained in RIPA when it was placed on the statute books in 2000.

The new powers provide a quasi-judicial veneer for the fact that various state agencies were already seeking far wider access to private data, and this is set to expand even further. A commentary by the civil liberties organisation Statewatch in 2003 had already noted that "hundreds of thousands of requests for access to communication data are already being made by agencies even though there is no legal power to do so."

According to a report this month by the civil and human rights group Liberty, there were "nearly 440,000 authorisations for communications data traffic between June 2005 and March 2006."

This massive extension of the state's powers to intrude into the life of the ordinary citizen was introduced without recourse to a debate in parliament but through the mechanism of a "parliamentary instrument" signed by the home secretary, Jacquie Smith, which one press report said was "quietly approved" in July.

The government claims to have held "full consultation" on the introduction of the new measures, but this is contested by those who follow civil liberties issues closely. Writing in the *Observer* newspaper, Henry Porter said, "Yeah, right. When? With whom? The Welsh Ambulance Service? The Postal Services Commission? Wychavon district council? All of them can now acquire your phone records. There was absolutely no debate about this, and it is nothing but a straight lie to claim otherwise."

"We are not intruding into people's private lives," a Home Office spokesperson said, going on to claim that the exercise of the new powers was consistent with the European Convention on Human Rights and UK Human Rights Act, as long as the demand for decryption is "both necessary and proportionate."

But who decides what is "necessary and proportionate"? And what public scrutiny is there to ensure that these powers are not being abused arbitrarily?

To require judicial approval for such a level of access requests would completely swamp the court system. So authorisation has been devolved to what Statewatch has called the office of the "toothless" Interception of Communications Commissioner, "which is hardly likely to engender public confidence."

"The holders of this post, and the Tribunal to which members of the public can complain about surveillance, were created under the 1985 Interceptions of Communications Act (now replaced by RIPA 2000), have never in the eighteen years of their existence upheld a complaint," according to Statewatch.

In a further Kafkaesque twist, those receiving a notice under section 49 of RIPA are legally prohibited from telling anyone apart from their lawyer about it.

Since 2004, telecom and Internet service providers have voluntarily provided data when requested; now, they will be required to retain such information for one year. However, since the provisions only apply to data within the UK, large corporations could easily avoid this by keeping their data and encryption keys offshore.

By 2009, the retention of data including Internet sites visited, emails sent and VOIP (Voice over IP or Internet telephony) will be mandatory.

This will put into UK law the highly contentious European Commission Directive on mandatory data retention, adopted in 2005, and will replace the current "voluntary" code introduced in the UK in 2003. This regulation does not just cover terrorism but all crime, however minor.

Not only in Britain but throughout Europe and internationally, the rights to free speech and personal privacy are being seriously eroded, with governments habitually citing the "fight against terrorism" to justify their mounting curtailment of long-standing democratic norms.

"Nothing to hide, nothing to fear" is the false mantra repeated by ministers of every political stripe.

But the latest extension of state powers in Britain through RIPA means historically determined democratic rights such as the presumption of innocence and against arbitrary state actions are being further abrogated. Such laws, enabling almost routine trawling operations through mountains of personal data by the state, weight the balance of power overwhelming in favour of "state rights" against those of the individual citizen.