British government rushes through emergency surveillance legislation

Richard Tyler
14 July 2014

The UK coalition government, with support from the opposition Labour Party, is rushing through emergency legislation maintaining broad surveillance powers ruled unlawful by the European Court of Justice (ECO).

The Data Retention and Investigative Powers Act (DRIP) is to be voted through both Houses of Parliament over just three days this week.

Conservative Party Prime Minister David Cameron justified the need for the emergency legislation by specifically citing "events in Iraq and Syria". He claimed that, "The ability to access information about communications and intercept the communications of dangerous individuals is essential to fight the threat from criminals and terrorists targeting the UK."

This is entirely bogus. The present debacle in the Middle East is a direct result of the policies pursued by the current coalition and previous Labour governments. Before the invasion of Iraq and the bolstering of the anti-regime forces in Syria by Washington and London there was no terrorist threat emanating from these countries. Moreover, the Western powers have been actively aiding and supplying Islamist jihadist opposition forces in Syria as part of their goal of regime-change.

Cameron could present no evidence for his assertion that the measures are necessary in the fight against terrorism, because there is none. Once again, the so-called "war on terror" is being employed to abrogate civil liberties and strengthen the repressive powers of the state.

The prime minister said the bill did not introduce "new powers or capabilities" but was about restoring "vital measures ensuring that our law enforcement and intelligence agencies maintain the right tools to keep us all safe."

His deputy, Liberal Democrat Nick Clegg, claimed the emergency laws would "not be used as an excuse for more powers, or for a 'snooper's charter'". Clegg even sought to present DRIP as protecting civil liberties.

All these claims are similarly mendacious.

In April, the European Court of Justice ruled that a European Union directive requiring telecom companies and Internet providers to retain phone, email and similar metadata for a period of between six and 24 months was an unlawful intrusion on personal privacy, and struck it down.

In a press release, the Court said the directive "entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data."

The Court listed three main objections to the directive. Firstly, that it covered all individuals, all means of electronic communication and all traffic data "without any differentiation, limitation or exception being made". Secondly, that it failed to establish any objective criterion to ensure access to the data could be used only for such offences that were serious enough to warrant such an interference with fundamental rights. Thirdly, in relation to the period of retention, that it made no distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued.

Far from simply maintaining existing powers now ruled unlawful by the ECJ, DRIP introduces new powers enabling data interception warrants to be issued covering companies based outside the UK, something that was not possible under the old legislation. Moreover, the bill requires "the retention of all data or any description of data", wording that can clearly mean more than just "metadata". Steve Peers, professor of

EU law and human rights law at the University of Essex, said, “The provision in the draft Bill to permit a requirement to collect ‘all’ data is inherently suspect, and it would certainly be a breach of EU law.”

“The government’s intention, as manifested by the bill, to reinstitute mass surveillance of telecoms traffic data is a clear breach of the EU Charter of Fundamental Rights,” he added.

Jim Killock, executive director of the Open Rights Group, said, “Blanket surveillance needs to end. That is what the court has said.”

Agreement to fast-track DRIP through Parliament was secured in private discussions between the party leaders. The use of the guillotine to curtail debate and the imposition of a party whip will ensure it passes without even the usual pretence of parliamentary “scrutiny.”

To secure the votes of the Liberal Democrats and Labour, the legalisation will contain a so-called “sunset clause”, by which it automatically expires at the end of 2016. However, past examples of such “temporary” legislation, such as the Prevention of Terrorism Act, show this to be worthless, as they were simply renewed each year by a compliant Parliament.

Promises of annual “transparency reports” and a “US-style privacy and civil liberties board” are merely sops to quiet the bill's critics in Parliament and the media. And they have had the desired effect, with the *Guardian* opining that the new law “provides an opportunity to introduce some civil liberties elements that up to now were missing.”

The emergency legislation has the effect of reinforcing the draconian Regulation of Investigatory Powers Act (RIPA), introduced under the previous Labour government. RIPA empowers nearly 600 state and public bodies to undertake covert surveillance.

The annual report of the interception commissioner, charged with oversight of RIPA, records some half a million surveillance notices and authorisations a year, as the wide-ranging powers are routinely used to spy on individuals, often for the most trivial infringements such as littering or dog fouling. Only a handful of challenges to the thousands of instances of surveillance have been upheld by the Investigatory Powers Tribunal, which meets in secret to conduct its “oversight.”

Under the new legislation, companies with data centres overseas can be forced to hand over information on their users’ online actions, giving the British state access to every Google search and Twitter or Facebook post. In this way, it is possible to build up the most intimate picture of a person’s online habits and acquaintances. All this data can then be trawled in a police dragnet.

Some press reports have claimed that the new law will clarify the position of foreign telecoms and Internet companies, giving them legal cover when they hand over customer data. However, there is little evidence that such companies have not cooperated fully with the British state. After all, Whitehall generously provides some £65 million to offset the cost of data retention.

According to the *Guardian*, “Downing Street insists this ‘extra-territoriality’ clause is not an obscure back door to provide legal cover for the Prism and Tempora data harvesting programmes revealed by Edward Snowden.”

But this is an entirely moot point. The activities of the Government Communications Headquarters (GCHQ) spy centre will not be covered by the new legislation, and the GCHQ will be able to continue its wholesale snooping on both UK and foreign citizens.