British government proposes extension of state surveillance

Paul Bond
11 April 2012

Britain's Conservative-Liberal Democrat government has announced plans to extend wider state surveillance across e-mail, telephone and social media communications. Senior government officials have made clear their determination to press ahead with these and other proposals that would strengthen the repressive apparatus of the state. These would include allowing secret court hearings in intelligence-related civil cases.

It was revealed earlier this month that the government is proposing the inclusion, in May's Queen's Speech, of a bill that would drastically increase the security services' scope for monitoring communications. The proposals would allow the government unprecedented access to personal communications and constitute a wholesale assault on democratic rights.

The government have been rather vague on the specific details of their proposals, suggesting that they will seek to implement whatever they can get away with.

Under existing EU legislation, Internet service providers (ISPs) have to keep details of users' web access, e-mail and Internet phone calls for 12 months. Content is not recorded, but details of sender, recipient, time of communication and geographical location are. At present, the data can be accessed by police and intelligence agencies without external authorisation, although access to content requires a warrant.

It is reported that the current proposals would allow the state communications intelligence agency GCHQ access to these data in real time, on demand, rather than retrospectively. It is not clear whether there are any plans for this access to require a warrant. It has been reported that the proposal is for ISPs to install hardware enabling GCHQ to access data on demand without a warrant.

The proposals would also extend the scope of the coverage to include social media sites like Facebook and Web-based telephone systems like Skype.

Security Minister James Brokenshire justified the real time access by appealing to the example of "rescuing someone whose life is at risk … not as part of some general snooping exercise". Under existing emergency rescue conditions the location of a mobile phone can already be traced after a request to the ISP or phone company. The current proposals, and Brokenshire's clumsy justification, suggest that this option will be made more generally available.

As criticism mounted of the proposals, Downing Street claimed that only these data would be accessible, not the content of any communications. Liberal Democrat MP Julian Huppert noted that all of the industry experts to whom he had spoken anticipated that this would hugely expensive and could not be done "without allowing access to the actual message that was sent—which is [currently] not legal without a warrant". Huppert, a member of the Commons Home Affairs Select Committee, said he had not seen "the details of these proposals—not for want of asking".

Deputy Prime Minister Nick Clegg sought to rescue the government from any criticism. Claiming to be "totally opposed" to blanket reading of emails he insisted that that was not the content of the plans. "All we are doing is updating the rules", he claimed.

As part of his rescue efforts he attempted to confuse the issue of the status of the proposal. Announcing the bill in the Queen's Speech would be to introduce it in the next parliamentary session. Clegg suggested instead that it would be circulated as a "draft bill".

This was a flimsy tactic, although it was sufficient to appease Liberal Democrat anxieties. Huppert called it "very important progress". Other government sources, however, were stressing to journalists that they were only prepared to tolerate minor delays as a sop to opposition. The Home Office insisted it planned to "legislate as soon as parliamentary time allows", and a senior source there said the plans "absolutely will not be dropped or even delayed".

Certain conciliatory noises have been made, with Cameron and Justice Secretary Ken Clarke saying they were willing to look at the details of both these proposals and the acceptance of secret court hearings. In the latter case, too, they have again indicated their clear determination to press ahead, using the moderate Liberal Democrat amendments to make it appear that they are taking civil liberties questions into consideration.

The Liberal Democrats have demanded that only a high court judge should be able to rule on a tribunal being held in secret. Clarke agrees with this position, saying he does not want the decision on trials going into secret session to rest with ministers.

There is general support for the idea. This is quibbling about the details. In fact, Clarke's insistence on the determining role of a judge has been questioned by the Joint Committee on Human Rights, which noted that the green paper does give the deciding vote to ministers. Under its proposals judges can only object to a decision on the grounds that it was irrational or disproportionate, not that it was wrong.

Clegg, similarly, has said that secret hearings should not be

extended to inquests. Clarke disagrees, saying that inquests cannot be treated differently.

The call for ministers to be able to authorise secret court hearings follows two legal defeats relating to Guantanamo Bay detainees. The government is anxious to avoid a repetition of incidents like the revelation of MI5 collusion with the US authorities in the torture of Binyam Mohamed. This was made public when the Court of Appeal ordered the release of a redacted summary of CIA documents.

This is not just a question of domestic repression. The British government is also keen not to upset its international allies. In 2010 the government paid £20 million (US$26 million) in compensation to 16 former Guantanamo Bay detainees rather than risk revelations about their treatment in open court.

Clarke has based his support for secret hearings on US reluctance to supply intelligence after the Mohamed ruling. “Sometimes national security demands that you have to give a guarantee of complete confidentiality to third party countries—and not just the Americans”, he said.

Clare Algar of Reprieve, the legal charity that represented Mohamed, described the secret hearings proposal as “a system in which they can use whatever evidence they like against the citizen, but the citizen is unable to challenge or even to see that evidence. This is unacceptable in any circumstances”.

The surveillance plan has been welcomed by Labour. Yvette Cooper, the shadow home secretary, called for an explanation of the proposals but expressed absolute agreement with the government’s line: “the police and security services need to be able to keep up with new technology to deal with serious issues including disrupting terrorist planning, catching paedophile rings or cracking down on organised crime”, she said. Ed Miliband’s chief complaint about the proposals was that they had been “spectacularly mishandled” by the government.

Labour’s support is hardly surprising. The last Labour government proposed a single giant database of all the UK’s web usage as part of its surveillance monitoring programme. They abandoned the idea in the face of opposition from the Tories and Liberal Democrats. Prime Minister David Cameron has said that the current plans are “not what the last government proposed”.

If anything the current proposals are even more draconian, with potentially constant access to personal data. Home Secretary Theresa May’s insistence that “There are no plans for any big government database” is entirely beside the point, as the proposals would give access to the same information.

The proposal has been justified on the grounds of helping the police “stay one step ahead of the criminals”, in May’s words. She argues for the move on the grounds that “currently online communication by criminals can’t always be tracked”. She also insisted that “Only suspected terrorists, paedophiles or serious criminals will be investigated”. Brokenshire claimed this was about solving crime, not “real-time snooping on everybody’s emails”. Brokenshire made clear that his only objection to such snooping was that it might be “disproportionate” to look at every Facebook conversation. The proposals, however, leave that option available.

Pointing to earlier use of communications data in securing the convictions of several high-profile child murderers, May said that “ordinary people” had nothing to fear from the proposals. This line has been trotted out by successive governments in justifying ever-increasing state surveillance of every aspect of daily life.

The innocent, of course, have the most to fear from such an escalation. Rather than proceeding from the presumption of innocence, which requires investigating authorities to demonstrate evidence justifying their surveillance, such measures place the burden of proof on the innocent. The measures, which would be used to police any dissent, are an escalation of the state monitoring of everyday life.

This is already at unprecedented levels. Under the last Labour administration surveillance was ratcheted up under the claims of monitoring terrorism suspects, but its application has been far wider. Under the Regulation of Investigatory Powers Act 2010 (RIPA), access to the surveillance data was made widely available to a number of agencies, including NHS Trusts, the Royal Mail and local councils alongside government departments, the police and intelligence services. Cases have been reported where councils have used RIPA powers to check on children’s school catchment areas.

In 2008 it was reported that an average of one in 78 British adults had been the subject of authorised surveillance. Estimates of the number of CCTV cameras in use across Britain range from 1.85 to 4.2 million. The vagueness of the figures is itself revealing of the scope and coverage of such surveillance. There are over 12,000 CCTV cameras in use on the London Underground alone.

The current proposals also highlight the token character of the supposed safeguards of democratic rights under parliamentary rule. A spokesman for the Information Commissioner’s Office told the press they were looking for “the implementation of the results of a thorough Privacy Impact Assessment”. Ultimately, however, “the decision as to whether to proceed with the project is one which has to be taken by parliament”.