# British parliament set to adopt law enforcing police access to encrypted email

**Mike Ingram**
**19 July 2000**

The Regulation of Investigatory Powers Bill (RIP) will be presented to the Commons for the final reading Wednesday after amendments made in the House of Lords.

Ostensibly introduced to regulate the investigatory activities of the state, under conditions of the rapid emergence of the Internet and email, the RIP bill makes massive inroads into democratic rights and civil liberties.

The Labour government is keen to get the bill written into law prior to Britain's signing of the European Convention of Human Rights (ECHR) in October, as much of the new law breaches the convention.

The RIP legislation requires Internet Service Providers (ISPs) to install a so-called "black box" device allowing access by the security forces to email messages hosted on an ISP's computers. The black box will 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 RIP bill also gives police the power to demand that those whose email is intercepted hand over any software keys and passwords necessary to read encrypted mail. Failure to do so could result in two years imprisonment. Telling a third party that such a request has been made carries a possible five-year sentence.

As with other law-and-order measures introduced by the Blair government, the draconian legislation has been justified on the grounds of thwarting "terrorists", "paedophiles" and "organised crime". Tucked away in part five of the proposed bill, however, in a section titled *Supplemental*, one finds a staggering indication of both the scope of the new powers and the legislation's real purpose.

Dealing with the "general interpretation" of the proposed law, the document explains that "serious crime" refers to crimes that satisfy two tests. The first is that the offence would carry a prison sentence of more than three years for anyone over 21 years of age.

The second reads as follows: "[T]hat the conduct involved the use of violence, results in substantial financial gain *or is conducted by a large number of persons in pursuit of a common purpose*" (emphasis added).

In the entire debate in the House of Lords and the media commentary surrounding the bill, little has been said about this clause and its implications for the population generally. The wording makes clear that the new legislation is designed to take account of any form of mass opposition to government policy and to give the security forces free rein to monitor such activities. To facilitate this, ISPs are to be recruited as police spies and anyone who does not quietly go along with this could find himself or herself in jail.

It is this reactionary political agenda that accounts for the government's determination to implement the new measures, despite concerns raised in business circles as to its effect upon the national economy, and the growing e-commerce sector in particular.

Many of the measures contained in the RIP bill were first set out in the Electronic Communications bill of 1999 but were removed after corporate representatives expressed concerns that the state surveillance of electronic commerce would be bad for business. At that time the government held a lengthy consultation period with ISPs. Now they have simply been informed they will receive partial reimbursement for installing the required equipment.

This has led some ISPs to threaten that they will move their servers abroad if the bill becomes law. The first to make such an announcement was Poptel, one of

the country's largest ISPs and service provider for the Trades Union Congress. The Poptel announcement was followed within hours by a threat from E-business infrastructure specialist Wellace. The company said it would withdraw all its commercial services unless the government redrafts the RIP bill. Another of the country's largest independent ISPs, Claranet, with over 350,000 subscribers, has said it will seriously consider moving some of its servers offshore unless the government amends its regulations.

Certain amendments to the new bill were discussed in the Lords but these were largely aimed at placating the ISPs and big business while leaving the thrust of the legislation intact. To this end, one of the first amendments passed was a proposal to specifically state that ISPs would be given fair compensation for the installation of a black box on their servers. Much of the criticism of government was that the £20 million price tag for implementing the proposals had massively underestimated the cost to ISPs.

Cosmetic adjustments were also made to the bill requiring that prosecutions must show that a person "knowingly" failed to comply with a decryption notice and that a body known as the Interception Commission must be notified within seven days of a demand for access to keys and passwords to decrypt mail.

Authorisation for key requests from police, Customs & Excise or the armed forces must now be signed at the rank of Chief Constable, Commissioner and Brigadier respectively, rather than "a senior officer" as stated in previous drafts of the bill.

A proposal that access to encryption keys require the authorisation of the Home Secretary, as an elected representative, was rejected by 120 votes to 119. Curbs on penalties for revealing a decryption notice were also rejected, allowing the government to impose a lifetime silence with a penalty of up to five years imprisonment for failure to comply.

If the legislation is passed in its final reading in parliament as is expected, Britain will become the only G7 economy with a law allowing government access to encryption keys. It is feared that the new legislation will have a dramatic effect upon the UK economy, as the Internet becomes an ever more significant factor in business.

Claranet systems manager Steve Rawlinson said in a company press release, "If growth in the use of the Internet by businesses for internal, business-to-business and business-to-consumer applications continues as forecast, then you can be sure that British jobs are going to be lost. For any international company, it really does not matter whether Internet services are based in France, Germany or the UK. It does matter to the UK economy—jobs will be lost or at least created elsewhere in Europe directly as a result of this legislation."

While a host of organisations exist to promote Internet freedom, their protests have done nothing to halt the passage of this legislation. Why is it that even the threat of a significant transfer of capital abroad has not altered the government's course?

To answer this it is necessary to understand the social context in which the Internet and related technologies have developed. The RIP bill and the controversy surrounding it reveal a fundamental problem facing the ruling elite. As the Internet and electronic commerce become increasing factors in the daily lives of millions of people and acquire a growing dominance within the business world, the political and state structures of a previous period become inadequate. While it is necessary for governments to promote the widest possible use of the Internet, they also recognise that its open character makes this technology an ideal vehicle for the widespread dissemination of critical opinions, political debate and protest.

The draconian character of the legislation being introduced in Britain is a reflection of the growing social divide within the country. A government that came to power pledging to take "class out of politics" has only succeeded in widening the gap between rich and poor. Under conditions of mounting social inequality and the inevitable political discontent this creates, the RIP bill is deemed necessary to maintain the long-term political and class interests of the ruling elite, whatever the immediate costs to the economy.