British Labour government to enforce police access to email encryption

Mike Ingram
31 March 2000

A bill going through the British parliament will give the security services and police extraordinary powers of surveillance over private emails.

The Regulation of Investigatory Powers Bill (RIP) has come under attack from the legal rights organisation Justice and the Foundation of Information Policy Research, among others. The two organisations warn that the bill, which includes granting the police powers to unscramble encrypted email, is likely to breach the European Convention of Human Rights (ECHR), which Britain is due to sign in October.

A legal opinion obtained from two leading lawyers, Jack Beatson QC and Tim Eicke from the Essex Court Chambers, criticises the government for opting for the widest police powers enabling open-ended interception of encrypted material. They say this "will have the inevitable consequence of compromising the affected individual's whole security and privacy apparatus" and is likely to contravene Article 8 of the European Convention on respect for private life.

Criticism is focused on Part III of the bill, which allows the police to serve written notice to demand that a communication be decrypted or a private encryption key be handed over. In a second "up-to-date opinion" issued by the organisations on March 22, a number of areas are cited where the bill could breach human rights laws.

Violation of the presumption of innocence:

Under the proposed bill, failure to comply with a decryption notice would be a criminal offence unless the person could prove they did not have the key, or access to it for any reason, such as losing the password. According to legal opinion, "This contravenes an important element of the fair trial right guaranteed by Art 6 ECHR: that it is for the prosecution to prove the offence, not for the defendant to prove his or her innocence.

Infringement of the right not to self-incriminate:

It is impossible for the police to prove by technical means that the defendant has possession of the key and the only way to prove a person ever had it would be by way of an admission by the defendant. "Furthermore, disclosure of the key may lead to the discovery of incriminating material. This contravenes a person's right to remain silent and not to contribute to incriminating him/herself as guaranteed under the fair trial right of Art 6 ECHR," Beatson and Eicke state.

Inadequate safeguards against abuse:

Not all decryption notices have to be authorised by a judge and there is no requirement that a notice be restricted to serious crime. Moreover, "There are inadequate safeguards on the holding of the decryption key and any material obtained. There is no requirement to inform the Covert Investigations Commissioner that such notices have been served. These are all requirements necessary to safeguard privacy rights under Art 8 ECHR," the lawyers point out.

Ostensibly designed to update existing legislation regarding the use of electronic surveillance in light of the development of the Internet, the bill not only makes massive inroads into democratic rights, but also allows the imposition of draconian prison sentences for anyone refusing to aid in its implementation.

The proposed legislation will designate Internet Service Providers (ISPs) as "public telecommunication systems". Paragraph 11(4) of the Bill makes its requirements binding upon a person "who has control of the whole or any part of a telecommunication system located wholly or partly in the United Kingdom". Employees of a company designated as offering a public telecommunications service will be obliged to obey surveillance warrants, or face a maximum of two years in jail. Section 18(2) of the bill says that employees could also face five years imprisonment for revealing the contents, details or even the existence of a surveillance warrant. There is no time limit on this requirement and there is no "whistle-blowing" clause (allowing employees to reveal practices that are considered to be against the public good).

Home Secretary Jack Straw has reserved the right to demand the placing of specific devices to monitor ISP traffic. What these devices will be is as yet unspecified.

Privacy campaigners have been quick to point out that with the emergence of the Internet, it is potentially as easy to gather information on the public as a whole as it is on an individual. Though the bill is ostensibly to regulate the powers of the security services, it gives them free reign to carry out mass surveillance.

Clause 8(1) of the bill sets out the requirement for warrants: "An interception warrant must name or describe either one

person as the interception subject; or a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place."

However point 8(3) states that warrants shall be named *unless*: "(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying (i) the descriptions of intercepted material the examination of which he considers necessary; and (ii) that he considers the examination of material of those descriptions necessary as mentioned in section 3 ..."

As long as the Home Secretary signs a certificate saying he is sure this is a matter of national security, the authorities can monitor whomever they want and no one will ever know about it.

Section 8(4) refers to "the interception of external communications in the course of their transmissions by means of a telecommunication system" as the condition under which the Home Secretary can sign a certificate. By "external communications" the bill means a message sent or received from outside of the UK. In this way, the security services have a mandate to monitor all traffic entering and leaving the UK, regardless of who it is addressed to or from whom it came. When considered in relation to the Internet, the potential scale of surveillance permitted by this clause is huge. Even where a message may not have originated outside the UK, it is highly likely that at some point in the journey through cyberspace, it was routed via an overseas network due to the congestion of internal routes.

Traffic data is the term used to describe the information that is gathered anonymously by ISPs, telecommunications companies and even web sites in the day-to-day use of their services. There has been increasing concern among privacy campaigners that this data could be made available for commercial purposes. The company DoubleClick was accused recently of planning the merging of data gathered through their web site with that from their newly acquired partners, the mail order firm Abacus Direct. Concerns focused on the fact that Abacus's database would put names and addresses to the traffic data acquired through the DoubleClick web site.

In the UK, legislation exists under the Data Protection Act to prevent corporate abuse of this data. The new Investigatory Powers Bill places no such control upon the use of the same data by government agencies.

Section 21(2) of the Bill gives an extensive listing of the grounds for obtaining traffic data: "in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder; in the interests of the economic well-being of the United Kingdom; in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health."

Finally, in case the authors of the bill forgot anything, Section 21(2) states that access to traffic data will be deemed necessary, "for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

The list of those able to obtain traffic data in section 24(1) is almost as long as the reasons for it to be collected. Ranging from a police force to "any of the intelligence services", the section again concludes with a catchall that includes "any such public authority ... as may be specified ... by the Secretary of State".

The Blair government is fast-tracking the bill. The first reading was on February 11 and the second on March 6. With a minimum of debate in Parliament it is expected to become law by October 4.

Many of the measures introduced in the RIP legislation were first drafted as part of the Electronic Communications Bill, but were removed after the business community expressed concerns that linking electronic commerce to questions of state surveillance would be bad for business. Whereas the Electronic Commerce Bill was subject to a certain consultation with Internet providers and others, no such process has been undertaken with RIP.

The development of the Internet poses a fundamental problem for the political representatives of big business. While it is necessary to promote the widest possible use of the Internet as business shifts towards it, the open character of this technology makes it an ideal vehicle for the widespread dissemination of critical opinions, political debate and protest. The significance of the Internet in the recent international protests against the World Trade Organisation has not been lost on government legislators and the security services.

Under conditions of growing social inequality and political discontent, governments around the world are rolling back long-established legal and democratic rights. The defence of Internet freedom and electronic privacy cannot be limited to Internet advocacy groups. It must be made an issue for working people everywhere.