Every phone call, email and internet click stored by 'state spying' databases

Every phone call, text message, email and website visit will be stored for a year for monitoring by the state.

By Richard Edwards, Crime Correspondent
Published: 9:00PM GMT 09 Nov 2009

Comments 95 | Comment on this article

Ministers had originally wanted to store the information on a massive Government-run database, but chose not to because of privacy concerns Photo: GETTY IMAGES

All telecoms companies and internet service providers will be required by law to keep a record of every customer's personal communications, showing who they are contacting, when, where and which websites they are visiting.

Despite widespread opposition over Britain's growing surveillance society, 653 public bodies will be given access to the confidential information, including police, local councils, the Financial Services Authority, the Ambulance Service, fire authorities and even prison governors.

They will not require the permission of a judge or a magistrate to access the information, but simply the authorisation of a senior police officer or the equivalent of a deputy head of department at a local authority.

Ministers had originally wanted to store the information on a massive Government-run database, but chose not to because of privacy concerns.

However the Government announced yesterday it was pressing ahead with privately-held "Big Brother" databases which opposition leaders said amount to "state-spying" and a form of "covert surveillance" on the public.

It is doing so despite its own consultation showing there is little public support for the plans.

The Home Office admitted that only a third of respondents to its six-month consultation on the issue supported its proposals, with 50 per cent fearing that the scheme lacked sufficient safeguards to protect the highly personal data from abuse.

The new law will increase the amount of personal data which can be accessed by officials through the controversial Regulation of Investigatory Powers Act (RIPA), which is supposed to be used for combatting terrorism.

Although most private firms already hold details of every customer's private calls and emails for their own business purposes, most only do so on an ad hoc basis and only for a period of several months.

The new rules, known as the Intercept Modernisation Programme, will not only force communication companies to keep their records for longer, but to expand the type of data they keep to include details of every website their customers visit – effectively registering every click online.

While public authorities will not be able to view the contents of these emails or phone calls – but they can see the internet addresses, dates, times and users of telephone numbers and texts.

The firms involved in keeping the data, such as as Orange, BT and Vodafone, will be reimbursed at a cost to the taxpayer of £2billion over 10 years.

Chris Grayling, shadow home secretary, said he had fears about the abuse of the data.

"The big danger in all of this is 'mission creep'. This Government keeps on introducing new powers to tackle terrorism and organised crime which end up being used for completely different purposes. We have to stop that from happening".

David Davis, the former shadow home secretary, added: "What is being proposed is a highly intrusive procedure which would allow Government authorities to maintain covert surveillance on public use of telephones, texts, emails and internet access."

He added that the permission to access the data should be granted by judges or magistrates.

"Whilst this is no doubt necessary in pursuing terrorist suspects, the proposals are so intrusive that they should be subject to legal approval, and should not be available except in pursuit of the most serious crimes," he said.

The Information Commissioner's Office also opposed the moves.

"The Information Commissioner believes that the case has yet to be made for the collection and processing of additional communications data for the population as a whole being relevant and not excessive."

Chris Huhne, the Liberal Democrat home affairs spokesman, has criticised the amount the scheme will cost for what is effectively "state spying".

He said yesterday: "Any legislation requiring communications providers to keep data on who called whom and when will need strong safeguards on access.

"It is simply not that easy to separate the bare details of a call from its content. What if a leading business person is ringing Alcoholics Anonymous?

"There has to be a careful balance between investigative powers and the right to privacy."

Ministers said that they have still got to work with the communications industry to find the correct way of framing the proposals in law – meaning it will not come before Parliament until after the General Election. But the Home Office yesterday insisted it would push the legislation through.

Jacqui Smith, then Home Secretary, originally launched a paper in April for consultation called "Protecting the Public in a Changing Communications Environment".

The responses, published yesterday, disclosed that more than 40 per cent of 221 respondents rejected it outright as the growth of the surveillance state.

Of those whose repsonses were considered, exactly half said that the proposed safeguards for the information to be stored were not adequate.

Only 29 per cent third supported the Government approach, whereas 38 per cent were against it.

Meanwhile the communications providers themselves questioned the cost of the scheme and whether it was even technically feasible.

The latest figures on the use of the RIPA legislation by public bodies, show that state bodies including town halls made 519,260 requests last year - one every minute - to spy on the phone records and email accounts of members of the public.

The number of requests has risen by 44 per cent in two years to a rate of 1,422 new cases every day, leading to claims of an abuse of using the powers for trivial matters such as littering and dog fouling.

Shami Chakrabarti, director of Liberty, said: "The Big Brother ambitions of a group of senior Whitehall technocrats are delayed but not diminished.

"We need a bold alliance of phone companies who fear losing public trust and concerned citizens to come together in opposition to these plans.

"If the authorities need to build up an intimate picture of a suspect's communications, they should have to go to a judge for a warrant.

"Law-abiding people have sustained too many blanket attacks on their privacy and they've had enough."

Alex Deane, Director of Big Brother Watch, said it was an "enormous and unwarranted intrusion into every aspect of our private lives" and said that the laws are in effect an "illiberal snoopers' charter."

John Yates, Britain's head of anti-terrorism, has argued that the legislation is vital for his investigators.

The Scotland Yard Assistant Commissioner said: "The availability of Communications Data to investogators is absolutely crucial. Its importance to investigating the threat of terrorism and serious crime cannot be ovetrstated".

Home Office Minister David Hanson said: "The consultation showed widespread recognition of the importance of communications data in protecting the public and an appreciation of the challenges which rapidly changing technology poses. We will now work with communications service providers and others to develop these proposals, and aim to introduce necessary legislation as soon as possible."

http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/6533107/Every-phone-call-email-and-internet-click-stored-by-state-spying-databases.html