# ISPA questions new Bill



**Nicholas Lansman**

Laws designed to gather communications data should keep pace with technological developments, but we are still to be convinced that current proposals are the most proportionate way of achieving this, writes Nicholas Lansman, Secretary General of the Internet Services Providers' Association (ISPA).

It is common knowledge that the government is looking to update its capabilities to capture and retain communications data. This is through the draft Communications Data Bill which is currently being scrutinised in Parliament. Although most will agree that law enforcement should be able to keep pace with modern forms of communication, the plans have been dubbed a 'Snooper's Charter' by some, and there has been significant opposition among campaigners, academics and others.

While it is claimed that the Bill seeks to maintain existing communication data capabilities, it appears that the powers contained in the Bill have huge implications for the UK communications industry and put the UK ahead of other countries in attempting to gather communications data in this way. Government has been working on proposals to enable law enforcement to keep track with technological developments and retain additional data for some time. As things currently stand, a number of CSPs retain certain types of communications data for up to a year and the legislation for this has developed over the past decade. The data in question is already held for business purposes, such as when an email is sent or a call made, and the law simply requires CSPs to retain this data for 12 months and to provide access for law enforcement.

The data does not contain the content of the communication as content can only be intercepted once authorised by the Home Secretary, whereas communications data only requires a senior officer's authorisation. Last year, police, security services and other law enforcement agencies made 494,078 requests for communications data.

The new proposals, if passed by Parliament, will require CSPs upon receipt of a notice from the Home Secretary to retain a great deal more data that is not held for business purposes such as third party data that crosses an ISP's network. Crucially, the communication protocols and data this is limited to will not be written into the legislation nor will the providers who are in scope be made clear. It is expected that applications like social media, webmail, VoIP and online gaming will be brought into scope but greater clarity is required.

The Home Office will be approaching foreign services providers and social networking sites directly to get access to communications data, and only if they refuse will CSPs in the UK be compelled to retain this third party data. The draft Bill hopes to give law enforcement the ability to use a filtering tool that will allow them to combine communications data profiles across different services and protocols, giving them a full picture of how people communicate. There is also an expectation that providers will need to ask for additional data, such as the details of new customers.

## Current state of play

As things currently stand a host of organisations can access communications data under various pieces of legislation. The Communications Data Bill will consolidate this within RIPA and also reduce the number of bodies with access to retained data to only the police, the Serious and Organised Crime Agency, the intelligence agencies and HM Revenue and Customs which are currently named on the face of the Bill. However, the Home Secretary will have the power to grant access to other bodies once the Bill has been passed and we expect that the list of bodies will increase again in the long run.

ISPA has been heavily involved in this area for more than 15 years and is working to ensure that the legislation is justified and proportionate. The Bill has huge implications for the UK communications industry with any public or private telecommunications company potentially being asked to retain data by the Government. We will be pushing for full cost recovery for ISPs and greater clarity over which providers are in scope and what the criteria for deciding this may be.

During discussions with members a number of concerns were raised, including whether privacy of users can be protected given the various ways people communicate, whether the filtering arrangements are proportionate, the implications to running networks, technical implications, and whether this is the most effective use of resources.

This is an ongoing debate and we will continue to consult with members on their views as well as provide written and oral evidence to the joint parliamentary committee. If you want to keep up-to-date with what is happening and what it could mean for your business please get in touch with us. ■
www.ispa.org.uk