



HOME SECRETARY

2 Marsham Street, London SW1P 4DF
www.homeoffice.gov.uk

Dr. Hywel Francis MP
Chairman of the Joint Committee on Human Rights
House of Commons
London
SW1A 0AA

13 June 2012

PUBLICATION OF THE DRAFT COMMUNICATIONS DATA BILL

The Queen's Speech on 9 May set out the Government's intention to: "bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital communications data under strict safeguards, subject to scrutiny of draft clauses". I am today publishing a draft Communications Data Bill which will be subject to pre-legislative scrutiny by a Joint Committee of both Houses and to a parallel inquiry by the Intelligence and Security Committee.

This legislation is needed to protect the public and bring offenders to justice by ensuring that the police, security and intelligence agencies can continue to operate effectively in the age of internet communications. The proposed legislation will update the legal framework to maintain vital access of these agencies to communications records (the "communications data") essential to solving crime in the 21st century. Communications data:

- is the information about a communication. It includes the time and duration of a communication, the number or email address of the originator and recipient and sometimes the location of the device from which the communication was made. It does not include the content of any communication;

- is already used by the police, security and intelligence agencies in the investigation of all types of crime, including terrorism. It enables the police to build a picture of the activities, contacts and whereabouts of a person who is under investigation. It is used as evidence in court across the UK every week;
- has played a role in 95 per cent of all serious organised crime investigations and every major Security Service counter-terrorism operation over the past decade;
- is already held by the communications industry. The police and others can only then access communications data on a case by case basis if they can demonstrate that access is necessary and proportionate.

Communications technologies and services are changing fast. More communications are now taking place on the internet using a wider range of services, such as voice over internet, online gaming and instant messaging. As criminals make increasing use of internet based communications, we need to ensure that the police and intelligence agencies continue to have the tools they need to do the job we ask of them: investigating crime and terrorism, protecting the vulnerable, and bringing criminals to justice.

The proposals will:

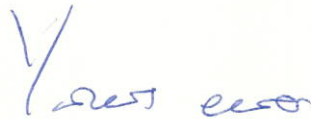
- require some communications service providers (CSPs) to obtain and store some communications data which they may have no business reason to collect at present;
- extend existing safeguards regarding data retention, access and oversight;
- replace dozens of currently available powers with weaker safeguards by a single piece of legislation, with oversight provided by the Interception of Communications Commissioner, and the Information Commissioner.
- ensure that four key bodies – the police, the Serious Organised Crime Agency/National Crime Agency, the intelligence agencies and Her Majesty's Revenue and Customs will have tightly controlled access to communications data. The other public bodies (including local authorities) who can currently access this data, will have no access unless Parliament agrees their use is vital to tackling crime and protecting the public.

In taking these proposals forward we will continue our long-established approach based on co-operation and collaboration with CSPs. We will not impose obligations on all providers or services, nor will we impose obligations without detailed discussions having first taken place. We will not require the collection of all internet data, which would be neither feasible, necessary, nor proportionate. And nothing in these proposals will authorise the interception of the content of a communication.

Without action there is a growing risk that crimes enabled by the internet will go undetected and unpunished. The impact on the ability of law enforcement and security agencies to protect the public would be significant. It is the duty of

Government to propose measures to tackle such a growing risk to public protection. The proposals in this draft Bill represent the Government's considered and focused response to this challenge. I recognise that these proposals raise important issues around personal privacy. I am committed to ensuring that here, as elsewhere, we get the balance right between protecting the public and safeguarding individual civil liberties. I welcome the process of pre-legislative scrutiny in ensuring that we have got this balance right.

Further information about these proposals (including a copy of the draft Bill) can be found at www.homeoffice.gov.uk If you would like a briefing with my officials on this subject then please contact them via DraftCommsDataBill@homeoffice.x.gsi.gov.uk or on 020 7035 0318.

A handwritten signature in blue ink, appearing to read 'Theresa May'.A handwritten signature in blue ink, appearing to read 'Theresa May'.

Rt Hon Theresa May MP