Home Office

James Brokenshire MP
PARLIAMENTARY UNDER SECRETARY FOR CRIME AND SECURITY
2 Marsham Street, London SW1P 4DF
www.homeoffice.gov.uk

20 AUG 2012

Rt Hon Dawn Primarolo MP
House of Commons
London
SW1A 0AA

CTS Reference: M10803/12
Your Reference: 01122333

13 August 2012

Dear Ms Primarolo

Thank you for your letter of 21 June to the Rt Hon Dr Vince Cable MP on behalf of your constituents who wrote to you to express concern about proposals for the collection and retention of communications data. I am replying as Minister for Crime and Security.

Communications data is the information, or the 'who, when and where' of 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 'what' – i.e. the content of any communication. Communications data is held by the communications industry. The police and others can access communications data if they can demonstrate that access is necessary and proportionate. Access is on a case by case basis and is subject to independent oversight. The police can get access to communications data only where it is connected to a specific investigation or operation.

Communications data is used by the police and the security 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 can be used as evidence in court. Communications data 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.

Comprehensive safeguards exist for access to communications data. It is primarily regulated by the Regulation of Investigatory Powers Act (RIPA), which places strict rules on when, and by whom, this data can be obtained. The Interception of Communications Commissioner, Sir Paul Kennedy, provides independent oversight of the acquisition of communications data. He provides a published annual report to the Prime Minister.

New communications technologies are generating communications data in different ways. Not all this data is currently retained by communications/internet service providers, as they may have no business interest in doing so; the police and others are therefore unable to get access to it. This has a direct impact on the investigation of crime in this country and on our ability to prosecute criminals and terrorists.

It is the first duty of Government to protect the public. In the Queen's Speech on 9 May 2012 the Government announced its 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 a draft Bill.

The draft Communications Data Bill was published on 14 June 2012 ahead of pre legislative scrutiny by a joint Committee of both Houses. The Intelligence and Security Committee will be conducting its own, independent, inquiry into the draft Communications Data Bill, as this is an area that impacts on the work of the intelligence agencies. Further information on the proposed bill (including the impact and privacy impact assessments to accompany legislation) can be found here: http://www.homeoffice.gov.uk/counter-terrorism/communications-data/index.html

The proposed legislation will help ensure the police can stay a step ahead of the criminals. But it will not:

- enable unfettered access by the police to data about everyone's communications
- provide the police and others with powers to intercept and read your emails, phone calls or check your contacts lists
- create a single government database containing your emails and phone calls to which the police and agencies can get unlimited and unregulated access
- weaken current safeguards or checks in place to protect communications data
- allow local authorities greater powers

The estimated economic cost of the programme in the period from FY2011/12 until 2015/16 is up to £800 million (this is the amount the programme would cost less inflation, irrecoverable VAT and depreciation).

It is difficult to estimate costs over the longer term: the programme has an incremental approach to developing capabilities, which responds to changes in technology and the communications market place. These changes are difficult to predict. Costs will be kept constantly under review and the business case will be refreshed on a regular basis.

Our current estimates are that the economic costs of this programme over ten years from 2011 could be up to £1.8 billion. Over ten years, we assess that this work will give measurable benefits of approximately £5–6 billion. This includes conservative estimates of direct financial benefits (assets seized, revenue lost etc). There are also benefits to which it is difficult to ascribe a financial value, for example seizures of drugs, disruption and prosecution of terrorists and improvements in operational efficiency.

An investment of £1.8 billion over ten years, or approximately £180m a year, amounts to just 1.3 per cent of the current annual £14bn policing budget.

We are proposing the following safeguards in the draft Communications Data Bill:

- Only four bodies – the police, Serious and Organised Crime Agency, Her Majesty's Customs and Revenue and the intelligence agencies – will be granted access to communications data through this bill. Other public bodies who currently have access to communications data will only continue to do so following debate and approval by Parliament and if that access is considered vital to protecting the public or investigating crime.
- Access to communications data will continue to be strictly controlled and will only be able to be obtained for a specific purpose (e.g. for the purpose of preventing or detecting crime, in the interests of national security or for the purposes of preventing death or injury in the case of an emergency) and by those public authorities authorised to do so.
- Following the Protection of Freedoms Act 2012, local authorities will now be required to secure judicial approval before obtaining communications data (or using any Part 2 RIPA technique). (The local authority provisions in the Protection of Freedoms Act will come into force in the autumn)
- The Interception of Communications Commissioner will continue to provide independent oversight of the acquisition of communications data by public authorities. The role of the Commissioner will also be extended to oversee the new powers, including the collection of communications data by communications service providers. This will include oversight of testing, regular auditing and inspections.
- Industry will be required to ensure that data retained is protected against accidental or unlawful destruction, accidental loss and unauthorised access or disclosure.

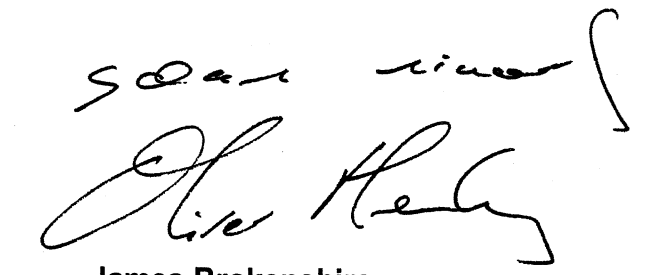
- Legislation will make explicit that all communications data retained by CSPs under the legislation will be destroyed after the 12 month retention period (unless required for legal proceedings).
- The legislation will provide for the Information Commissioner to keep under review the security and integrity of the communications data retained e.g. against accidental loss, unlawful destruction, unlawful retention and unauthorised disclosure, consistent with the Data Protection Act. There is also provision for the Information Commissioner to keep under review the specific requirement to destroy data when its retention is no longer lawfully authorised (e.g. at the end of a retention period specified under the new provisions).
- If a communications service provider is concerned about the requirements placed upon them, they can ask an independent Government / Industry body (The Technical Advisory Board) to consider the impact of these obligations. The Technical Advisory Board would then advise the Secretary of State on whether the obligations should be maintained, modified or removed.
- The role of the independent Investigatory Powers Tribunal (made up of senior judicial figures) will be extended to cover the new provisions ensuring that individuals have a proper avenue of complaint and independent investigation if they think the powers have been used unlawfully.

In short: there will have to be good reason for Government to require both the collection and storage of communications data. The Government set out its intention to legislate on this issue in the Strategic Defence and Security Review (SDSR) which was published in 2010. The SDSR made clear that we would legislate as soon as parliamentary time allowed, ensuring that the use of communications data is compatible with the Government's approach to civil liberties.

The police and other authorised public authorities can only access communications data for the permitted purposes which are set out on the face of the Bill. These purposes have to be approved by Parliament and essentially relate to the investigation of crime.

It is impossible to know in advance of a crime taking place or a criminal investigation opening whose data will need to be investigated and whether those people are suspects or victims. In order for the police and others to be able to access data when they need it, for example to investigate a murder or locate a person at risk, the data has to have already been retained – if it has not been retained, it cannot otherwise be retrieved and access to it is not therefore possible. The data that has been retained by CSPs will then only be accessed by authorised public authorities on a case by case basis and where this relates to a specific operation or investigation.

We wish to maintain a capability not increase it.



p.p. **James Brokenshire**