Background and History of the Communications Data Bill and the Need for a Home Office Consultation on the draft Communications Data Bill

"Before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups … Meaningful consultation can take place only once there is clarity as to the real aims of the Home Office, and clarity as to the expected use of the powers under the Bill."
Joint Committee on the Draft Communications Data Bill's Report, 11th December 2012[1]

Open Rights Group has made a call for organisations and individuals to contact the Home Office to ask for a consultation on communications data and the Communications Data Bill. This document sets out where the draft Communications Data Bill came from, provides some background of the key issues and outlines why another consultation is necessary.

Organisations and individuals who want to ask the Home Office for a consultation can use this form to contact the Home Office.

What is Communications Data?
In the draft Communications Data Bill, the Government defines communications data as:
"information about a communication; it can include the details of the time, duration, originator and recipient of a communication; but not the content of the communication itself."[2]

This means that for an email, the email addresses of the sender and recipient, the time it is sent and the location it was sent from is included. The content of the email is not communications data. For a telephone call, the number of the caller and the time and place of the call is communications data but the content of the call is not included.

Currently, the principal piece of UK legislation concerning communications data is the Regulation of Investigatory Powers Act 2000. This allows the police, intelligence and security services, HM Revenue and Customs as well as hundreds of other public bodies to access communications data held by telephone, postal and internet providers. This includes users' name, address, phone calls they make and receive, the source and destination of emails and mobile phone locations. The UK Government intends to update and extend these powers with the Communications Data Bill.

Communications Data under the last Labour Government
The UK Government has been working towards producing a Bill on communications data since at least 2006. This process was started under the last Labour Government and continued by the Conservative and Liberal Democrat coalition since their election in 2010. The most recent consultation on communications data was published by the Home Office in April 2009. The Home Office did not published a response to that consultation. There has not been a public consultation on communications data since then.

The Interception Modernisation Programme
The last consultation on communications data in 2009 was as part of the Labour Government's Interception Modernisation Programme (IMP). This was an initiative within the Home Office looking

[1] http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf
[2] http://www.parliament.uk/documents/joint-committees/communications-data/CM208359DraftCDBill.pdf

at which further capabilities the government should have for intercepting and storing communications data.

The then Prime Minister Gordon Brown said in February 2008 of the IMP, "*communications technology is changing rapidly; there is a switch towards internet protocol communications, with the clear implications that that brings for our security. Accordingly, we have launched the interception modernisation programme to update our capability to ensure that, under those new circumstances, our national interests will continue to be protected*."[3]

According to Vernon Coaker, Minister of State at the Home Office, in November 2008, "*the objective of the Interception Modernisation Programme (IMP) is to maintain the UK's Lawful Intercept and Communications Data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost*."[4]

Again according to Vernon Coaker in November 2008:
I recognise there is a difficult balance between public safety and public rights to privacy so I recently announced my intention to launch a public consultation on the Interception Modernisation Programme... The consultation document ...will set out the range of background issues including the vital requirement of communications data in protecting the UK from serious crime and terrorism, the need for a solution to maintain our capability and the need to provide adequate safeguards as part of any solution."[5]

The Government's position was that people were increasingly communicating using the internet. In order for law enforcement agencies and the security services to protect public safety and to combat serious crime and terrorism effectively, there would have to be changes in the law to allow them to access this new data. Because these changes were likely to be controversial, the Government decided to run a public consultation.

The April 2009 Consultation

The Labour Government published a consultation on communications data in April 2009.[6] It laid out

1. what communications data is and how it is used under RIPA,
2. how uses of technology are changing and why that will impinge on the ability of public authorities to protect the public and investigate crime and
3. three possible approaches on what the law regarding use of communications data should look like.

The Government did not support the first two options, which involved either storing all communications data on a single database or, in their words, 'doing nothing'.

The Government's preferred approach, which it called "a middle way," was to have communications service providers "*collect and retain communications data relating to their own services but also collect and store the additional third party data crossing their networks*." This data would be accessible by public authorities on a case-by-case basis subject to certain safeguards.

[3] http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080206/debtext/802060004.htm#08020693000193
[4] http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm081119/text/81119w0032.htm#08112012001081
[5] http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm081124/text/81124w0005.htm#0811249000549
[6] "Protecting the Public in a Changing Communications Environment", 2009, http://www.officialdocuments.gov.uk/document/cm75/7586/7586.pdf

In December 2009 following the end of the consultation, Labour dropped plans to introduce legislation on communications data. The Parliamentary Under-Secretary of State for the Home Office Lord West announced that "plans for legislation are not developed sufficiently for it to be included in this Session of Parliament." [7] The Home Office did not publish a response to the April 2009 consultation and so it is not entirely clear what the precise reasons were for the plans being dropped. There was however very widespread opposition to the plans amongst industry. A Freedom of Information request by technology news site *The Register* showed that every major UK mobile network company and large numbers of internet service providers registered strong objections to the Government's plans in the April 2009 consultation.[8]

Communications Data under the Conservative and Liberal Democrat Government

By July 2011 the new Government had published its Counter-Terrorism Strategy, which included plans to:

"*introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communications data and also to intercept communications within the appropriate legal framework. Legislation will be brought forward to put in place the necessary regulations and safeguards to ensure that the response to this technology challenge is compatible with the Government's approach to information storage and civil liberties*."

The draft Communications Data Bill was announced in the Queen's Speech in May 2012,[9]with a Bill published in June 2012.

Because the proposals were controversial, a Joint Committee of twelve members drawn equally from the House of Commons and the House of Lords was formed to look at the detail and make recommendations on how the Government should proceed. They took written and oral evidence from the Home Office, the police, civil liberties groups, academics, journalists, internet service providers and others.

The Draft Communications Data Bill

The Communications Data Bill would allow the Secretary of State to order 'telecommunications operators' to retain, for a period of 12 months, communications data relating to their subscribers that they would not otherwise keep.[10]

The collection of communications data on behalf of the government is to be done on a national scale. Every person who uses the internet in the United Kingdom would have details such as the websites they visit, people who they communicate with and when they communicate with them stored for a year. Information about every person in the United Kingdom, regardless of whether they have committed a crime, will be obtained, stored, and potentially accessed by public authorities.

The Bill provides a framework for obliging selected companies to collect data which they would not normally need, for the Government's benefit. Currently, companies are only required to retain and grant access to data they generate for business purposes.

[7] http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/91210w0003.htm#09121056000226

[8] http://www.theregister.co.uk/2009/12/22/mobile_imp/

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62226/Queens-Speech-2012briefing-notes.pdf

[10] Part 1, §1 & 4(1), Draft Communications Data Bill 2012

Under the draft Communications Data Bill, organisations which could access communications data would include: police forces, the intelligence and security services, the Serious Organised Crime Agency, and HM Revenue and Customs (HMRC). Other authorities are included in the Bill. In addition, the Home Secretary could add any other public authority to that list.

These organisations would designate a person to grant authorisations to access the data.

What is a 'telecommunications operator'?

The Bill states that a telecommunications operator is anyone who operates a service which exists "*wholly or partly... for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy*."[11] In other words, the Bill covers telephone networks and ISPs. Businesses, including those who provide social networks, forums, webmail, and internet voice calls, are also treated as telecommunications operators.

In principle, the draft Bill would also cover overseas telecommunications providers although United Kingdom legislation does not have direct effect outside the United Kingdom's jurisdiction. Clause 1(3)(c)(ii) of the draft Bill would require telecommunications providers in the UK to store and disclose information from third party services traversing their networks.

What data will be collected?

Communications Data as defined in the draft Bill includes three types of information: traffic data, use data or subscriber data.

The term "traffic data" is defined within the Bill as any data "*compromised in, attached to or logically associated with a communication for the purposes of a telecommunications system...and which identifies, or purports to identify, any person, apparatus or location to or from which the communication is or may be transmitted*."[12]

Subscriber data is defined as "information held or obtained by a provider about those to whom the service is provided". Use data is defined as "the use made by any person of a postal or telecommunications service, for example, itemised telephone call records or itemised records of connections to internet services"

Communications data would therefore include, for example, the list of persons to whom a Facebook status update may be communicated, because a friend list is "*data...logically associated with a communication...which identifies any person to which the communication...may be transmitted.*" It includes the usernames of people communicating with each other over Skype. It includes lists of members of private Facebook groups. It also includes the time, date, and physical/electronic location of the device through which all of these example communications are made.

Communications data are not supposed to be content of a communication. However, we argue that the data covered by the Bill can still be very intrusive. The observation that someone repeatedly contacts Narcotics Anonymous, or Gaydar or a political website, even without seeing exactly what they look at, gives a detailed insight into their character. By combining email, telephone, web access, social network data, and mobile phone location history, one may deduce a detailed and intimate picture of someone's movements, habits and beliefs.

[11] Part 3, 28(1) "telecommunication system", Draft Communications Data Bill 2012 12
Part 3, 28(2) "traffic data" - *Ibid*

Why the data can be used

The draft Bill says that the ten permitted purposes for which communications data can be requested are:

- in the interests of national security,
- for the purpose of preventing or detecting crime or of preventing disorder,
- for the purpose of preventing or detecting any conduct in respect of which a penalty may be imposed under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse),
- 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,
- to assist investigations into alleged miscarriages of justice, or
- where a person ("P") has died or is unable to identify themselves because of a physical or mental condition— ◦ to assist in identifying P, or
    - ◦ *to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.*

Different public bodies will be able to access information for certain of these purposes.

Searching the Data and Profiling Individuals

It would not be possible for humans to search through the vast amount of retained data. So the Bill contains provisions for establishing 'filtering arrangements.'[12] This is referred to as a 'Request Filter.'

These provisions would create, in effect, a search engine[13] accessible by police forces, the intelligence and security services, the Serious Organised Crime Agency and HM Revenue and Customs. Information would be combined from the databases of many individual telecommunications operators, social networks, webmail providers and internet voice calling providers into a single database.

The Joint Committee explained in its report how the filter would be used by citing the evidence of ISP association LINX:

"*it would be technically possible to "perform profile searches of the following format: 'List all persons who are the designated user of a mobile phone that was in Location (e.g. Trafalgar Square) at Time (e.g. noon last Tuesday), and who have read any of the following websites more than once in the past period (e.g year)' "*."

In its written evidence to the Joint Committee, the Home Office gave this example as to how the filter would work:

"*During a live terrorist investigation, if a law enforcement agency wanted to identify a suspect who they know was at two separate locations at two specific times, they might currently need to submit*

[12] Part 2, §14-16, Draft Communications Data Bill 2012

[13] Communications Data Bill creates 'a virtual giant database' http://www.bbc.co.uk/news/uk-politics-18884460

separate requests to obtain a full list of all those devices at each location, then compare these lists to see which one was in both locations."

Open Rights Group presented the following example of how the filter might be used in its written evidence to the Joint Committee:
"*the data could identify a protester who posts to a radical politics site, and their location at any given time. Their favoured contacts, those likely to be politicised and their locations could be identified. The data could in effect be used to monitor political activity, or any activity deemed unusual or deviant, to a finely grained level*."

Safeguards
The Bill offers some "safeguards". For example, organisations such as the police will nominate an internal 'Designated Senior Office' (DSO) and a 'Single Point of Contact' to authorise access to the collected data of millions of people. The Joint Committee described the way the system would work: "*Before the application* [to use the request filter] *reaches the DSO it is channelled through a Single Point of Contact (SPoC) who is a trained expert, independent of the investigation, who will advise the applicant and the DSO on whether the application is necessary and proportionate, what collateral damage may result and whether the communications data sought is likely to be available*."

Each year the Interception of Communications Commissioner (IoCC) and his inspectors review a subset of the applications to ensure that policy is being applied correctly. The process also relies upon public bodies voluntarily reporting errors to the IoCC.

The IoCC inspects the system for access to communications data to ensure it is done in accordance with the law. They also make recommendations on how to improve the system when errors occur. This is to reassure the public that intrusion into privacy is kept to a minimum. He also review the Home Secretary's use of interception warrants, the investigation of encrypted electronic data and the adequacy of these safeguards.

Open Rights Group's view on the draft Communications Data Bill
Open Rights Groups' views on the draft Communications Bill are available to read in their submission to the Joint Committee on the draft Communications Data Bill and their response to the Joint Committee's report.

The Joint Committee on the draft Communications Data Bill
A Joint Committee of six members from the House of Commons and six members of the House of Lords was set up in July 2012 to consider the Bill. They received evidence from the Home Office, the police, civil liberties groups, academics, journalists, internet service providers and others. Their report on the Bill was published on 12th December 2012.[14]

Whilst recognising that legislation was necessary, they concluded that the Bill pays "insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should." The Committee also called for "a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups."[15]

The Joint Committee made a number of recommendations. They said that the Bill should be significantly amended. Under the draft Bill, the Home Secretary would be able to extend the types of

[14] http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf
[15] http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf

data that communications service providers would be obliged to retain without a need for new legislation. This is with the intention of 'future-proofing' the law so that the police and security services can adapt to investigatory needs. The Joint Committee said that the Home Secretary should not have this power and that there should be new primary legislation if the Home Secretary wanted to have more types of data retained.

The report also said that Government should consider the importance of allowing communications service providers to remain competitive and aim to minimise the extent to which the reputation of the United Kingdom as being open to business is damaged. They also say that the Government should bear in mind that smaller CSPs may be particularly burdened by complying with the Bill.

The Joint Committee said that the draft Bill does provide protection of internet users' communications data. They added that storing web log data carries the possible risk of databases being hacked into or accessed by the wrong people with potentially damaging consequences.

The Joint Committee's Call for a new consultation on the Communications Data Bill

The Joint Committee's report criticised the Home Office strongly for not having consulted prior to publishing the draft Bill:

"*The Home Office should not have assumed that a consultation paper published in April 2009 could justify publication of draft legislation three years later without further consultation with the public and with those most closely affected by its proposals. The evidence we received shows that United Kingdom CSPs were not given any details about the possible content of notices before the draft Bill was published, overseas CSPs were not consulted about the draft Bill at all, nor was there any further public consultation.*"

The Joint Committee called for a new consultation on communications data and the Communications Data Bill before a new Bill is published. It also went into significant detail about a large number of areas on which the Home Office ought to consult further:

"*Before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups. This consultation should be on the basis of the narrower, more clearly defined set of proposals on definitions, narrower clause 1 powers and stronger safeguards which are recommended in this report. The United Kingdom and overseas CSPs should be given a clear understanding of the exact nature of the gap which the draft Bill aims to address so that those companies can be clear about why the legislation is necessary....Meaningful consultation can take place only once there is clarity as to the real aims of the Home Office, and clarity as to the expected use of the powers under the Bill.*"

The Joint Committee recommended that the Government should consult on whether all ten purposes for which the draft Bill says communications data can be requested are necessary. The draft Bill allows for the Home Secretary to add new purposes by order. The Joint Committee thought that if the Home Secretary wanted to add further purposes in future, that should require primary legislation.

They also thought there should be a consultation on the definitions of subscriber data. The Bill's current definition could currently be understood as covering data that social networks keep on their customers which can be very personal and not usually considered to be communications data. They suggested that the definition of subscriber data "*should include checks on the name, date of birth, addresses and other contact information held on the subscriber to a communication service; for each service the customer's unique ID (e.g. mobile number, e-mail address or username); the activation,*

suspension and termination dates of an account and payment and billing information." The Joint Committee said that the language of RIPA is out-dated and that there should be a consultation with industry on how communications data should now be defined. The definitions of communications data in the draft Bill are based on the definitions in the Regulations of Investigatory Powers Act 2000 (RIPA).

The Joint Committee's report notes that the Government has no legal authority to compel overseas providers to generate or store communications data. It says that there should be consultation as to whether the Bill should contain measures for the Government to *ask* overseas providers to retain more data and for Government to help with the costs for those providers to do so.

The Joint Committee said that the Home Office should "*examine whether it would be technically and operationally feasible, and cost effective, to require CSPs to keep web logs only on certain types of web services where those services enable communications between individuals*." The Home Office would have to consult with communications service providers and experts to work out whether this would be feasible.

The Need for a new Consultation on Communications Data

The Home Office responded to the Joint Committee's report by saying, "*The Home Office has considered the Joint Committee's recommendations carefully and accepts the substance of them all. In light of this the Bill is currently being re-drafted and the Home Office plans to engage with interested parties on our proposals in the coming weeks*."

Unfortunately, the Home Office has not carried out the consultation proposed by the Joint Committee. The Home Office is proceeding with re-drafting the Communications Data Bill but has not released details of what measures the new Bill will contain or the date when it will be published. It has not carried out a rigorous and extensive and public consultation on the Bill from a range of sources outside the Department following the publication of the Joint Committee's report.

It is important that the Joint Committee's recommendations are taken on board by the Home Office. As the Joint Committee pointed out, the gap between the last consultation on communications data in 2009 and the publication of the draft Communications Data Bill is too long. As a result, the voices of a number of key stakeholders – not least the general public – are not being heard or taken into account.

Open Rights Group would like people and organisations with an interest in communications data and the Communications Data Bill to be consulted by the Home Office. If you have a view as to whether there should be a new Home Office consultation on communications data and the Communications Data Bill, we ask that you contact the Home Office to inform them of your view.

If you want any more information or have any other questions about the Communications Data Bill, feel free to contact Open Rights Group at campaigns@openrightsgroup.org