Communications Data Bill briefing note

Open Rights Group. June 2012.

What's happening?

In the 2012 Queen's Speech the Government announced that they would “bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital communications data under strict safeguards to protect the public, subject to scrutiny of draft clauses.” The published draft Bill is called the **Communications Data Bill.**

We believe that as it is currently written the Bill would mean a substantial increase in the powers the state has to order any communications provider – whether it is an Internet Service Provider (ISP) like BT or an Internet company like Google – to collect, store and provide access to our information about our emails, online conversations and texts. We are concerned about the way that the data is gathered and the rules governing who can access it and why. The draft Bill is problematic on both counts; we believe too much information will be collected and that there will be inadequate safeguards around access to it.

What does the Bill say?

The draft Bill contains three parts:

- **Part 1** of the bill creates a new power to order companies to collect specific datasets, creating them if necessary, and deploying any technical or policy changes needed to do so. It also requires this data to be retained in a secure and confidential manner for 12 months, and destroyed after this period elapses. This power can be used by any principal secretary of state (which means most cabinet ministers), but in practice would be the Home Secretary. Use of this power must be ratified by a vote in Parliament.[1]
- **Part 2** of the bill creates a system for assorted public bodies to get access to this data.[2]
- **Part 3** makes some changes to the 'Regulation of Investigatory Powers Act' (RIPA), repeals all other existing powers that involve retaining and disclosing "communications data", and makes the Information Commissioner, the Interception of Communications Commissioner, and the Investigatory Powers Tribunal responsible for scrutiny and oversight of the implementation of these powers.[3]

What is the problem? The key issues

1. General surveillance of the population

The government is giving itself extremely broad powers to, effectively, order any communications provider to collect and disclose communications data by almost any means. The government hasn't said how collection might work, even though the way the data is collected is critical. It is most likely to involve 'black boxes' being installed on ISPs networks, which will harvest communications data which can then be access by relevant government bodies. That represents a fundamental shift to general, mass surveillance of the population - outsourced to the private sector.

Communications providers will be required to collect a lot of data that currently they do not. That means that the proposals will lead to the creation of a distributed (meaning, 'it's not all in one place') database of a wide range of information about our communication.

2. This does more than 'maintain' existing powers

Communications data can paint a very intimate picture of our lives. The data generated through our use of services like Facebook, Google and Twitter tells people far more about us than phone records – it reveals our our tastes, preferences and social 'map'. Furthermore, the distinction between 'content' and

1 http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft/Commentary#Part_1:_Ensuring_or_Facilitating_Availability_of_Data

2 http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft/Commentary#Part_2:_Regulatory_Regime_for_Obtaining_Data

3 http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft/Commentary#Part_3:_Scrutiny_and_Other_Provisions

'communications data' does not, in practice, easily hold.[4] So to claim this is simply an 'update' of existing powers is not accurate.

3. It will be too easy to access the data

For law enforcement purposes, access to the data will simply require designated senior officers at those bodies to believe that it's "necessary to obtain the data" and that it is "proportionate to what is sought to be achieved." That effectively means that there will be no external, meaningful and direct oversight of access requests. We believe this will be ripe for abuse and exploitation. The safeguards over access need to be tightened up. The phone hacking scandal and subsequent revelations of the Leveson Inquiry help to demonstrate that the ability to access personal information will be exploited for a variety of reasons.

4. Filtering and 'fishing'

The clauses on "filtering" appear from the drafting notes to be applied to identifying data associated with an individual from a query across datasets or databases. However, the technical ability to search and identify people will go much further, and will be hard to regulate. For instance, 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 to a finely grained level, even in something close to real time.

There may be a small number of possible sources for a leak of confidential data in the public interest. Identifying the ways they communicate and identities (mobile phone, Facebook account, second phone) would be easy. Even an anonymous phone would retain the same or similar location data, so could be associated back to the person. Comparing the individuals that might leak data with the journalist publishing the story's contact details would reveal the likely leaker. As currently drafted we see no means in the Bill to restrict such queries and requests. Such judgements would be made by the police alone.

5. Why is it necessary?

The Government needs to explain clearly who it is that does not currently have access to what information, and explain exactly who need these new powers and why. It is not enough to simply say that the police need this information to solve serious crimes, without providing evidence or detail to substantiate that claim.

6. How much will it cost?

The Government estimates this scheme will cost £1.8bn. There is little to substantiate that figure, or any explanation of the ongoing costs of upgrading and maintaining equipment.

What needs to happen now?

This is a draft Bill. It will be debated over the next 6 months, with a joint committee of MPs and Lords reporting back by the end of November. Either the Bill needs to change substantially, for example to include specifics about how data will be collected and warrants for access to the information, or the Bill must be dropped completely.

For more information please contact Jim Killock: jim.killock@openrightsgroup.org or 020 7096 1079

Some key reading

1. **Full draft of the Communications Data Bill:** http://www.official-documents.gov.uk/document/cm83/8359/8359.asp
2. **ORG commentary and key questions about the draft Bill**: http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft/Commentary
3. **Analysis of the draft Bill from barrister Francis Davey**: http://www.francisdavey.co.uk/2012/06/communications-data-bill-first-look.html
4. "**The draft Communications Bill is a wasted opportunity**", Privacy International https://www.privacyinternational.org/blog/the-draft-communications-bill-is-a-wasted-opportunity
5. **"Briefing on the Interception Modernisation Programme",** LSE, 2009, http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

4 http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf