Investigatory Powers Bill

On Monday June 27th, we urge you to participate in the Second Reading debate on the Investigatory Powers Bill (IP Bill).

The IP Bill sets out the powers the intelligence and security agencies, the police and other government bodies have to collect and analyse vast amounts of Internet data.

Open Rights Group does not believe that this significant Bill was scrutinised or amended sufficiently by the House of Commons.

Below is a short briefing on the Bill. For more information, please contact us at any time: Jim Killock, Executive Director: jim@openrightsgroup.org 07894 498 127.

Key concerns with the Investigatory Powers Bill

- **Internet Service Providers (ISPs) and telecoms companies will be forced to collect detailed information about what everyone does online**, including our Internet histories and app use. The Home Office's estimates for collecting and keeping this information secure have been disputed by Internet Service Providers.
- **Internet histories can be accessed by the police without judicial authorisation.** They will only need internal sign off.
- **Data from phones, and Internet records could be data mined by the police**, through a "filter". This power could enable the police to engage in fishing trips.
- **There are powers to hack networks and computers**, including "bulk hacking" of unidentified machines. GCHQ, MI5 and the police will be able to hack people or companies who are not under suspicion. This is a routine measure, lacking special restrictions, rather than an exceptional power.
- **The intelligence agencies will be able to retain and examine copies of entire 'bulk personal datasets' held by private and public organisations.** The examples given in the Bill are the electoral roll or the telephone book. It could also include everyone registered with the NHS or people attending a specific event. These datasets would be combined and used for sophisticated automated analysis. Warrants to get hold of these datasets will last for six months.
- The Bill includes vague powers to compel communications providers assist with surveillance demands, including **removing "electronic protections"**. In some cases this might require that companies compromise their software to make the encryption less effective. This could have severe consequences for everyone's Internet security.
- **The parliamentary committees that analysed the Bill made 123 recommendations for changes**. They were concerned about the economic impacts, poor definitions and the lack of proper "operational cases" for the powers. The majority of these have been not been properly dealt with in the revised Bill.
- **Authoritarian regimes will pass similar laws.** The Bill's impact will reach beyond the UK as other countries pass similar laws. The Chinese Government said it took inspiration for its much-criticised terrorism law from the the US and UK.

Internet Connection Records and the Request Filter

ORG believes that proposals for Internet Connection Records and the Request Filter should be removed from the IP Bill.

Internet Connection Records (ICRs)

The IP Bill incorporates the proposals from the last Parliament's draft Communications Data Bill, also known as the 'Snoopers' Charter'. These will force telecoms companies to generate and store Internet Connection Records (ICRs). Nobody has been able to fully explain what exactly ICRs are. These are broadly described as a list of apps and websites that customers have visited, but not specific pages within a website (for example alcoholics-anonymous.org.uk/ not alcoholics-anonymous.org.uk/AA-Meetings).

No other democratic country collects its citizens' web browsing history. Existing "data retention" of more limited Internet records has stopped in about half of Europe, including Germany. There is yet to be a single study that convincingly shows that police data retention is effective. Even the European Commission, deeply attached to data retention measures, can't find any convincing evidence.

Costs of ICRs

The Home Office has said that the cost to ISPs for collecting ICRs will come to £174.2 million over ten years; BT say that this would cover their costs alone. The Internet Service Providers Association said that they *"do not recognise"* this figure. The Science and Technology Committee has warned that uncertainty about costs, *"risks undermining the UK's strongly performing Tech sector"*. Costs may well spiral, as the amount of data collected increases and with the filtering necessary to make sense of it and the measures to keep it secure from criminals.

The Request Filter

The Request Filter is described by the Home Office as a safeguard designed to reduce the collateral intrusion produced in searching for small, specific information in a large dataset. In reality, the Request Filter would allow automated complex searches across the retained data from all telecommunications operators without any judicial authorisation at all.

This has huge privacy risks. Even the Food Standards Agency will be able to self-authorise itself to cross reference people's Internet history with mobile phone location and landline phone calls—and search and compare millions of other people's records too.

Open Rights Group is the UK's only grassroots digital rights campaigning organisation.

www.openrightsgroup.org