OPEN RIGHTS GROUP

INVESTIGATORY POWERS BILL

– GUIDE FOR ORG SUPPORTERS

The Investigatory Powers Bill (IPB) will give extensive surveillance powers to the UK's law enforcement and intelligence agencies. It will replace other surveillance laws, including parts of the Data Retention and Investigatory Powers Act (DRIPA) and parts of the Regulation of Investigatory Powers Act (RIPA).

This is happening in part because of the Snowden revelations, which led to three inquiries into surveillance in the UK. Each of these inquiries recommended that a new, clear and comprehensive law on surveillance should be passed.

The IPB will put the surveillance capabilities revealed by Edward Snowden into statute. It will also increase mass surveillance by forcing ISPs to collect and keep a record of all the apps and websites that their customers visit.

The draft Bill was scrutinised by three parliamentary committees who between them came up with 123 recommendations. Lawyers, journalists, the tech industry, activists and academics have also criticised the Bill. However, the Government published the revised Bill with very few changes and is now trying to rush it through Parliament.

WHAT'S IN THE BILL?

➔ Bulk collection

The IPB outlines the full mass surveillance powers available to the security services as revealed by Edward Snowden. There has been no attempt to restrain these powers. The security services can use warrants to intercept bulk communications and collect vast amounts of communications content and data. Tapping undersea fibre-optic cables, GCHQ can record and keep all passing Internet traffic for several days, and metadata for six months.

Surveillance should be targeted: Bulk collection on this scale is mass surveillance. We are calling for a number of provisions in Part 6 of the IPB to be removed or amended to ensure that surveillance is targeted, based on suspicion, necessary and proportionate.

➔ Bulk personal datasets

Under the Bill, the intelligence agencies would 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.

Surveillance should be targeted: The intelligence services should not be able to examine and analyse records of millions of people who are not under suspicion of any crime. Access to any personal datasets should be authorised through more targeted warrants, based on suspicion and signed by a judge.

➔ Data retention and bulk collection for law enforcement

The IPB 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).

The police and other government organisations (such as the Department of Health) will be able to access and analyse these records through a 'filter'. Effectively, all of our communications and location records from ISPs and phone companies would become part of a single, searchable, distributed dataset. The Government claims this is a privacy enhancing measure, as only the results of the complex and powerful searches need to be presented to investigating officers.

ISPs are already forced to keep communications data about your emails, telephone calls and Internet access. This data can be accessed by police, government organisations and local authorities.

Surveillance should be targeted: Data retention in the UK is already intrusive. The IPB will extend this further making the UK the only EU or Commonwealth country to retain people's Internet browsing history. The creation of ICRs requires such an intrusive monitoring of Internet communications that it would be tantamount to interception. The Science and Technology Committee said that the lack of clarity about ICRs could put the UK tech sector at risk. The creation and retention of ICRs and the centralised search 'filter' should all be removed from the Bill.

➔ Hacking (equipment interference)

The IPB clarifies the powers of security agencies to break into our computers and mobile phones, including worrying new powers for non targeted mass hacking. The Bill also forces Internet companies to help the security services to hack their customers – for example by pushing out malware that will infect devices.

The IPB will give security and law enforcement agencies – including organisations such as HMRC – the powers to hack into devices of people based in the UK. The security services will be given 'bulk equipment interference' powers to hack devices or networks outside of the UK. This can include hacking people or even entire organisations, who are not under suspicion in order to reach targets.

The state should keep the Internet secure: Hacking can make the Internet less secure for everyone. As we saw with the Gemalto and Belgacom hacks, hacking can have serious consequences for individuals and companies who are not suspected of any crimes. We want to introduce amendments to the Bill that will ensure that hacking will be targeted and used only in the most extreme circumstances, with stringent independent oversight of the techniques used.

➔ Encryption

The Government is sending out very confusing messages about encryption. The Bill mainly carries forward existing arrangements for the government to access encryption – with no changes for individuals applying their own crypto. However it also creates vague new powers to compel communications providers to 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.

The state should keep the Internet secure: Companies should not be forced to make the Internet less secure. We will ask for these confusing and dangerous provisions to be removed from the Bill, and substituted with clearer clauses that protect secure communications from interference.

WHO WILL SIGN OFF SURVEILLANCE WARRANTS?

The Home Secretary has claimed the new system has a 'double lock' for interception and bulk warrants. This means that warrants are signed by a Secretary of State, then further authorised by a Judicial Commissioner. The Commissioner will not assess the grounds for the application, but simply whether the Secretary of State acted in good faith and followed the due process. Judicial Commissioners will be serving or former High Court judges, but here they would not be acting in that role; and it is highly unlikely that they would challenge a decision under such a narrow remit. If they do, the Secretary of State can ask their boss - the Investigatory Powers Commissioner - to decide whether to approve the decision to issue the warrant. This is rubber stamping, not proper judicial authorisation.

Warrants for the acquisition of communications data – call records, Internet histories, etc – will still be signed off internally without any judicial involvement. This is the process for a long list of public bodies – including HMRC and the Food Standards Agency – but not local authorities, which need to go to a judge.

Authorisation should be independent: We will call for the Bill to be amended so that independent serving judges at the appropriate level can decide whether surveillance is necessary and proportionate not just whether procedures have been followed. This is the system in the US, Canada, Australia, New Zealand and many EU countries.

WHO WILL OVERSEE SURVEILLANCE?

The Intelligence and Security Committee (ISC) will continue to provide parliamentary oversight. They have been criticised before for their 'cosy' relationship with the intelligence agencies.

A new Investigatory Powers Commissioner (IPC) will replace a number of commissioners who provide independent oversight of surveillance decisions.

The IPC will be in charge of the Judicial Commissioners that "authorise" certain types of surveillance warrants, and it would also have expanded capacity to report to Parliament and the public.

A simplified oversight regime is positive and the Bill states that it will have dedicated legal, technical and communications support. Even if independent serving judges were responsible for signing warrants, an independent commissioner could help with technical issues and improve compliance, transparency and accountability. However, it is problematic that both authorisation and oversight will fall into its remit. The IPC must be truly independent and not involved in the authorisation of surveillance if it is to genuinely audit the implementation of surveillance. Judicial Commissioners will both authorise warrants signed by the Secretary of State and audit those surveillance warrants. ORG will call for these functions to sit within separate bodies.

WHAT CAN YOU DO IF YOU HAVE BEEN UNDER SURVEILLANCE?

The new Bill will allow a domestic right of appeal from the Investigatory Powers Tribunal, which is something that ORG has called for.

It is difficult for individuals to seek redress if they have no way of finding out if they have been subject to surveillance.The IPC will have the power to inform individuals who have been the subject of serious errors by law enforcement and the security and intelligence agencies. This is a positive step. However, it does not go far enough.

Surveillance should be as transparent as possible: Anyone who has been subject to surveillance should be legally notified as long as there is no risk that this would jeopardise an ongoing investigation. Ideally this should happen within a year of the conclusion of an investigation.

Find out more about more at openrightsgroup.org/ipb

OPEN RIGHTS GROUP

OPENRIGHTSGROUP.ORG