
Introduction

The Government’s draft Investigatory Powers Bill (IP Bill) sets out, for the very first time, a comprehensive list of the investigatory powers that have been, or will be once passed, granted to the police and security services. As techUK has called for in the past, the Bill brings together all of the powers already afforded to law enforcement and the security services to obtain and intercept communications data. Along with a number of factsheets, impact assessments and explanatory notes, the draft Bill represents an unprecedented attempt by the Government in creating a world leading, modern framework for surveillance.

One of the reasons why the Communications Data Bill (2012) failed to pass was due to a lack of consultation with industry. It is reassuring that a number of measures that industry were concerned with in 2012 did not reappear in the IP Bill, such as third party data retention. However other measures, such as the requirement for companies to retain Internet Connection Records (ICR), have been kept in and it is important that these provisions are scrutinised, debated and properly understood.

techUK’s detailed response to the draft Bill proposes a series of questions that must be considered by the parliamentary committee that will scrutinise the draft Bill in order for it to meet standards on necessity, proportionately and effectiveness.

Key Issues

- Draft Bill includes a clear strengthening of the oversight regime for investigatory powers, however falls short of the recommendation by David Anderson QC that all warrants be authorised by a judicial commissioner

- Draft Bill includes a public avowal of capabilities such as bulk collection and equipment interference; capabilities that were until now lawful under very broad powers

- A significant change in the draft Bill is the obligation for Communication Service Providers (CSPs) to retain internet connection records (ICR) – a record of the internet services a user has accessed such as a website or instant messaging app

- The Government has been at pains to stress that it is not seeking a ban on encryption and that CSPs will be required to take "reasonable" steps to made data available under warrant.
Oversight and authorisation

On initial reading, one of the most striking aspects of the draft IP Bill is the clear strengthening of the oversight regime for investigatory powers. The draft Bill puts forward a proposal to create an independent Investigatory Powers Commissioner (IPC) – a senior judge responsible for approving the authorisation of interception, bulk collection and equipment interference warrants (unless in urgent cases) and overseeing how the investigatory powers afforded to the security services are used. Under RIPA, the Interception of Communications Commissioner (one of three oversight Commissioner roles to be merged into the IPC role) is appointed by the Prime Minister. The Prime Minister will also appoint the IPC.

The strengthening of the oversight regime is a step in the right direction, as one of the main criticisms of current surveillance practices is that the oversight arrangements in place do not provide adequate protections through the involvement of an authority separate from the investigative apparatus, authorising, approving and reviewing warrants. The involvement of a judge in the authorisation process for interception warrants brings the UK closer to other democratic nations and is also an important step in facilitating international co-operation between like-minded, democratic countries.

However, it should be noted that the IPC will only be able to “approve” interception, bulk collection and equipment interference warrants, and will not be responsible for authorising such warrants. This falls short of the recommendation by the Independent Reviewer of Terrorism Legislation, David Anderson QC, who stated that all warrants (apart from those relating to foreign policy or bulk warrants) should be authorised by a judicial commissioner.

According to the draft IP Bill, a judicial commissioner must review the “process” of the warrant being issued and base their approval on whether the warrant is “necessary” and “proportionate to what is sought to be achieved”. It is important that the role of the judicial commissioner is not procedural and merely that of a judge “rubber stamping” interception warrants. The joint parliamentary scrutiny committee should question how strong the role of the IPC will be and the grounds as to which a judicial commissioner can refuse to approve an interception warrant.

Transparency

The greater transparency evident in the Bill, including the public avowal of capabilities such as bulk collection and equipment interference, is also welcome since it will help rebuild public understanding and confidence in surveillance practices.

Alongside the draft Bill, the Government also published its first annual transparency report; a guide to the range of investigatory powers, the extent of their use and the safeguards and oversight in place to guard against their abuse. This includes statistics on, for example, the number of communications data requests that were made in 2014 and follows advice that techUK made in our briefing paper on the upcoming Bill.

Communications Data and Internet Connection Records (ICR)

A significant change in the draft Bill is the extension of the definition of “communications data” to include internet connection records (ICR) – “a record of the internet services a specific device has connected to, such as a website or instant messaging application”. These will have to be retained by the company providing access to the internet for up to 12 months, along with other types of communications data listed in current legislation.
The Government has been keen to stress that this will not be an individual’s full internet browsing history, but rather a record of the services that they have connected to. These records would therefore include, for example, a record of the fact that a smartphone had accessed a particular website or app at a particular time. Along with IP address resolution, which featured in the Counter Terrorism and Security Act (2015) and is maintained in the draft IP Bill, it is argued that internet connection records will be crucial for identifying the sender of a communication.

Access to internet connection records will be more tightly controlled than for other communications data as local authorities will be prohibited from accessing them. However, along with other types of communications data, law enforcement will be able to access an individual’s internet connection records through a communications data acquisition notice and not a warrant signed by a judge. Access to internet connection records will therefore be authorised by a Designated Person, independent from the particular investigation but within the same public authority.

Anderson, in his review, argued that internet connection records should only be included in the draft IP Bill after the operational case has been put forward for its need, with a rigorous assessment made of its effectiveness, intrusiveness and potential cost. The Home Office has followed his advice and published an operational case for internet connection records alongside the Bill.

When assessing the proportionately, effectiveness and need for the retention of internet connection records, the joint parliamentary committee must scrutinise the operational case that has been made and also question whether initial judicial authorisation should be required for a power as intrusive as accessing an individual’s internet connection records.

The committee should also consider whether the £175m that the Government has budgeted for the retention of ICRs is sufficient, in light of the vast amounts of data that companies will be expected to keep, as well as understand the technical challenges of separating “metadata” from “content”, as the draft Bill demands.

**Equipment Interference**

The draft Bill also makes provisions for a more explicit equipment interference regime that will govern how the security services interfere with electronic equipment, such as smart phones and computers, in order to obtain data.

According to the Bill, the definition of “equipment” includes any equipment “producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment”. The definitions stated in the draft Bill are relatively broad, and as the use of Internet of Things (IoT) products and services increase, the parliamentary committee will need to get a clearer definition of the scope of products that will fall under the definition of “equipment”.

Equipment interference and computer network exploitation can be highly intrusive investigative activities that may have repercussions to the security of devices and network infrastructure affected, ranging from using the login credentials of a target to gain access to the data held on a computer to remotely installing a piece of software on to a device or network in order to gain access. It can also potentially affect innocent consumers using a service or network. Understanding how these powers are used and the safeguards in place...
to protect innocent consumers, such as the requirement for Equipment Interference warrants to only come into force after judicial approval, is key to ensuring that confidence remains in the security of equipment and software.

The draft Bill also sets out the safeguards and provisions that are in place to ensure that such powers are not abused. However it also lays out the “duty” on CSPs for giving effect to an Equipment Interference warrant, stating that companies “must take all steps to give effect to the warrant”. Although the Bill caveats this by stating that companies should not be required to take steps that are not “reasonably practical”, it is important that the parliamentary committee scrutinise the requirements that are placed on CSPs in relation to equipment interference and ensure that companies are not forced under legislation to weaken the security of their own products or networks.

**Bulk Collection**

The draft Bill also includes a public avowal, for the first time, of the security services’ bulk collection powers. Although current legislation provides for the acquisition of data in bulk, the draft Bill puts on a statutory footing all of the bulk powers available to the security services.

Once again, warrants for bulk collection will need to be approved (but not authorised) by a judge before coming into force. Furthermore, in relation to warrants that affect overseas operators, the Secretary of State authorising the warrant must not only consult the operator affected but also take into account the likely number of users that may be affected, the technical feasibility and likely cost of complying with any requirement that may be imposed on a company. The explanatory notes supporting the draft Bill make it clear that any costs incurred by a company in complying will be reimbursed by the State, but it remains important to understand the scope and scale of such requests.

All of the safeguards above are provisions that techUK have called for in the past, along with the requirement that the operational case for bulk collection is made if the Government wish the capability to continue. It is important that the operational cases made in the draft Bill for bulk collection are critically examined in order to ensure that the capability is proportionate, necessary and effective.

**Obligations on Communications Service Providers**

As the Home Office has stated, the provisions laid out in the draft Bill require the co-operation of CSPs, both in the UK and overseas. For this reason, it is important that the draft Bill provides clarity to companies as to their legal obligations to help the security services in their vital work.

Whilst that clarity is partly provided by the fact that all of the obligations placed on companies has been brought together under one single piece of legislation, further information is required as to any wider assistance that may be expected of companies and the costs associated with maintaining permanent capabilities for the security services, for example. In particular, the joint committee should question the estimated costs on CSPs for storing new communications data such as internet connection records.

Furthermore, whilst it should be welcomed that overseas companies will not be required to retain communications data under the draft Bill (taking account of any potential conflict of laws that overseas companies may face), the draft Bill will still require overseas companies to comply with interception warrants, mutual assistance warrants, communications data
acquisition notices, equipment interference warrants and bulk warrants (interception, acquisition and equipment interference). Interception and communications data powers rely on overseas providers, however techUK has been clear that the draft Bill should not reassert UK law extraterritorially since this would likely trigger reciprocal action from other governments and not achieve the government’s policy goal of greater legal clarity.

Reforming the Mutual Legal Assistance Treaty (MLAT) process, and creating international agreements with like-minded nations, are the only sustainable, long term solutions to addressing complex legal conflicts and gaps between jurisdictions, as highlighted by Sir Nigel Sheinwald, the Prime Minister’s Data Sharing Envoy. It is important that the Government builds on Sheinwald’s work and creates a new international framework to prevent companies facing irreconcilable conflicts of law. It is only through this reconciliation that the IP Bill can deliver on its intentions in creating a workable legal framework.

**Encryption**

The Government has been at pains to stress that it is not seeking a ban on encryption and that Communications Services Providers will be required to take “reasonable” steps to made data available under warrant. The implications of the draft Bill for the use of end-to-end encryption appears to depend upon maintenance of the current interpretation of what is reasonable and a determination of whether end-to-end encryption is applied by the CSP or the user. However, the government has been very clear that its intent is not to restrict the use of encryption and we will be paying close attention to ensure this remains the case.

**Next steps**

The challenge now is for the draft Bill to be properly scrutinised by a Joint Committee of Parliament in order to ensure that it meets the standards of necessity and proportionately. Despite the comprehensive nature of the draft Bill and the supporting documents released by the Home Office, a number of questions still remain. techUK will be consulting widely with our membership to ensure that there are no unintended consequences for the draft Bill that the Home Office may not have considered. We will be submitting the views of our members to the parliamentary committee in addition to a range of other engagement activities.