Internet Telephony Services Providers' Association

The draft Investigatory Powers Bill

IMPORTANT: If the draft Bill is passed in its current form, only companies that have been served with an appropriate data retention notice will have to implement changes in order to remain compliant. Those without will only have to produce information if they hold it already.

ITSPA Position

The ITSPA Council has discussed this issue at length. The consensus opinion is that the proposed legislation would not involve any change to the current proceedings for the majority of ITSPA members and only relevant if a member is served with a data retention notice (as stated above). Members who are also ISPs should remain vigilant of the implications as well. There are theoretical issues surrounding the definition of ICRs, the issue of accessing encrypted data and extraterritorial concerns all which require further clarity. These have all been raised by the relevant Parliamentary Committee reports (see below) and the issues are being championed by various organisations (including ISPA and techUK) who are more closely affected. ITSPA will continue to monitor the progress of the Bill and engage if deemed necessary.

The draft Bill

The Investigatory Powers Bill was published on 4th November 2015. The Bill and associated documents can be found here.

Overview:
Introducing the Bill in the House of Commons on the 4th November, the Home Secretary stated that the Bill would:

- Consolidate and upgrade powers with 'world class' safeguards and provide a modern, legal framework based on openness and transparency
- Be different from the draft Communications Data Bill of 2012 with no third party retention by UK CSPs, no requirements for US companies to meet UK retention requirements and no ban on encryption
- Be scrutinised by a Joint Committee with a revised Bill in Parliament in the Spring and new powers in place by end of 2016

- Focus on three areas: interception, communications data and equipment interference
- Create a new powerful IP Commissioner bringing together the various existing bodies that will ensure strong oversight

Timetable:

- The Parliamentary Joint Committee held its final evidence session with the Home Secretary on 13th January.
- The Committee announced a call for written evidence on 1st December which closed on 21st December. The full list of written evidence received is available here.
- The Committee published its report on the draft Bill on **11th February 2016**. The Committee is expected to receive a response from the Government within weeks rather than months.
- The revised Bill is expected to be presented to Parliament in **early March** and will come into force by the **end of 2016 –** this is a priority for the Government due to the sunset clauses in DRIPA and RIPA.

Key aspects of the Bill

Internet Connection Records:

When announcing the draft Bill in Parliament, the Home Secretary said the challenge was to ensure that where once the police could get access to a missing child through mobile communications, this is not always the case for internet-based communications. Therefore, ICRs were needed to address this gap.

ICRs were described as a record of a communication service a person has used. For example, it would only record a 'communication service website, illegal website or IP address data' accessed, not the content or a news or medical website, akin to an itemised phone bill. People are referring to this as "weblogs" but actually it means IP addresses and ports.

At ITSPA's meeting with the Home Office in November, we were assured that an internet telephony voice service provider would not generate internet connection records and the requirement for these to be retained would therefore not apply. The requirement would, however, apply to an ISP but not to a pure voice service provider. However, it should be acknowledged that there are no provisions in the draft Bill which guarantee this and this was simply an assurance that the Home Office gave to ITSPA.

A Government factsheet specifically on ICRs is available here.

Retention & Interception of Communications Data

As far as ITSPA understands, the draft Bill does not change the Government's existing position regarding the retention of communications data**. A CSP is not obliged to retain data unless they have had a retention notice served on them by the Government.**

Currently, before a retention notice is served, a pre-review process is carried out between the Home Office and the CSP to establish what exact data is required and what is technically possible for the CSP to provide – the Home Office has stated that this process will remain in place.

Despite some speculation to the contrary, the Home Office emphasised that there is no intention under the Bill to serve more retention notices on smaller CSPs and acknowledged that, generally, it is mainly the largest providers who are subject to retention notices.

The current system, whereby CSPs can apply for funding from the Home office if compliance with a retention notice requires new equipment/staff etc, will remain.

In the case of intercept, where a CP has to change its systems to comply with an order the Home Office will pay the CSP's costs in doing this.

The following Government factsheets of relevance have been published:

- Targeted interception
- Bulk interception
- Communications data general
- Communications data request filter
- Bulk communications data

Extra-territorial application

All those who provide a UK communications service will be bound by the legislation and UK law applies across the world. However, the Home Office have acknowledged that there are only three areas of the Bill for which the Government has international enforcement powers:

- Targeted interception
- Bulk interception

- Acquisition of communications data

This is not a change to the current status quo and, notably, the Government does not have international enforcement powers regarding the retention of communications data. They continue to rely on the good will of the law enforcement bodies and overseas companies when making specific requests om overseas providers.

There is also no legal requirement on US companies to meet UK retention requirements.

Encryption

Despite much media speculation on the subject before publication of the draft Bill, the Government has stated it is not making any attempt to 'ban' encryption. The Home Office have stated that the Bill does not change the Government's existing position on the subject.

Regarding end-to-end encryption, the Home Office are aware of the difficulties concerning encryption which has been initiated by the end user and that the communications provider may not have the technical capability of decrypting such communications. The Home Office have stated that, if a CSP claims that they do not possess the required key and cannot decrypt a communication, the matter would have to go to court for a judge to determine what is reasonable.

At her oral evidence session with the draft Bill Joint Committee the Home Secretary, Theresa May MP, reiterated that the Government is not interested in undermining encryption and acknowledged its importance for businesses. However, she stated that if a CSPs were to be served with a warrant, they would be expected to provide the information requested in a readable form. At the session, May did not provide any further clarity on what the draft Bill would mean for end-to-end encryption. There are still ambiguities in this area which we hope will be resolved by scrutiny.

Authorisation & Oversight

Current situation regarding authorisation:

- Interception by law enforcement agencies and intelligence agencies requires authorisation by a Secretary of State with Judicial Commissioners providing retrospective oversight.
- Bulk acquisition of communications data requires a warrant authorised by a Secretary of State.

Future authorisation situation:

- The so called 'double-lock' authorisation for bulk interception, communications data and equipment interference warrants, requiring approval from a Secretary of State and Judicial Commissioners.

Current oversight situation:

- A number of bodies provide oversight for law enforcement and intelligence agencies:
    - Parliament's Intelligence and Security Committee
    - The Interception of Communications Commissioner's Office (IOCCO)
    - The Intelligence Services Commissioner
    - The Office of Surveillance Commissioners (OSC)
    - The Investigatory Powers Tribunal (IPT)

Future oversight situation:

- The current structure of three Commissioners who oversee investigatory powers exercised by public authorities will be consolidated into one body – the Investigatory Powers Commission – which will be headed by the Investigatory Powers Commissioner.
- The IPT will provide a new strengthened right of redress to individuals who believe themselves to be unlawfully subject to investigatory powers.
- The ISC will remain as a Parliamentary Committee with the right to scrutinise all the work of the intelligence agencies.

Other aspects of the draft Bill

The draft Bill also includes measures concerning equipment interference. The Government has published two factsheets outlining the draft Bill's measures in this area:

- Targeted equipment interference
- Bulk equipment interference

Committee Scrutiny

Three Parliamentary Committees have scrutinised the Draft Investigatory Powers Bill. Summaries of their findings can be found below:

Internet Telephony Services Providers' Association

Joint Committee on Draft Investigatory Powers Bill

The **Joint Committee on the Draft Investigatory Powers Bill**, chaired by Lord Murphy of Torfaen, was formed to scrutinise the draft Bill, the powers it contains and the authorisation and oversight regimes which should ensure that the powers contained in the Bill are properly used.

The Committee held its first oral evidence session on 30th November and concluded taking evidence on the 13th January, its final witness being the Home Secretary Theresa May MP. The Committee published its report on 11th February and the Government will respond to this in the coming weeks.

The Committee's report has made 86 recommendations, which it says are aimed at "ensuring that the powers contained in the Bill are workable, can be clearly understood by those affected by them and have proper safeguards". The key recommendations from the Committee include:

- **Encryption**
  - The drafting of the Bill should be amended to make it clear that backdoors will not need to be installed on systems.
  - The Government needs to make explicit that CSPs offering end-to-end encrypted communications or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so.
- **Internet Connection Records (ICRs)**
  - Although there is a case for ICRs as an important tool for law enforcement, the Home Office must address concerns about the definition and feasibility of the existing proposal. It is also important for ICRs to be properly authorised and overseen.
- **Bulk powers**
  - If included in the final Bill, a fuller justification for each of the bulk powers should be published alongside the Bill.
- **Data Retention**
  - Industry should receive 'whatever financial and technical support is necessary' as data will not be being held for business purposes.

Intelligence and Security Committee Report

On 9th February the Intelligence and Security Committee published its report on the Bill. The report, which heard from the Home Secretary and heads of the intelligence and security agencies,

focuses on the agencies' use of investigatory powers and made a number of clear and strong criticisms of the draft Bill. The Committee stated that the draft Bill:

- Does not place all the agencies' powers in one place and is a 'missed opportunity' in this regard.
- Should include an entirely new section dedicated to protecting privacy as this should be an integral part of the legislation rather than an add on.

On communications data, the Committee added that:

- The approach to the examination of communications data is currently 'inconsistent' and 'largely incomprehensible' and the same safeguards should be applied to all communications data – e.g. currently bulk acquisition warrants have fewer safeguards to obtain communications data.
- Agencies have a range of capabilities that could be used to obtain equivalent ICR data and so ICR measures in the draft Bill will mostly used by law enforcement. The legislation should make this clear.

Science and Technology Committee Report

Separately, following a one-off evidence session on the draft Bill, **the Science and Technology Committee** began an inquiry into technology aspects of the draft Bill. The inquiry held two evidence sessions, with witnesses including senior executives from ISPs, academics and civil servants among others. The inquiry has now concluded and the Committee's report was published on 1st February.

The report stated that the Bill 'risks undermining the UK's strongly performing tech sector because of uncertainty about the costs of complying with the new legislation'. Additionally, the Committee stated that this risks placing UK businesses at a relative commercial disadvantage to overseas competitors. More specifically, the Committee highlighted the following areas of concern:

Definitions – The Committee state that a number of important terms in the Bill are poorly defined, including Internet Connection Records (ICRs), resulting in confusion over the scope and costs of implementing the proposed measures. Additionally, they state that the terms 'removal of electronic protection' and 'equipment interference' are poorly defined, creating further uncertainty.

End-to-end encryption – The Committee highlighted that there is still a lack of clarity in this area, particularly on what steps a CSP should take when decryption of a communication might not be possible if it had not added the original encryption. The Committee calls on the Government to clarify that it will not be seeking unencrypted content in such cases.

The full Committee Report can be read here.

Reaction to the draft Bill

Labour:

- The Shadow Home Secretary, Andy Burnham MP, welcomed the introduction of the draft Bill in November 2015, saying that the laws were outdated, and law enforcement could not have investigative blindspots. He added his support for Government activity to update and create a 'world class' framework through stronger safeguards.
- Since then Burnham has changed his stance on the Bill with him and Keir Starmer MP, who is leading the Party's work on the draft Bill, calling for the safeguards contained in the legislation to be strengthened.
- On February 11th, Burnham and Starmer published a letter calling for the Government to take time to reconsider the draft Bill and take into account the findings of the three Parliamentary Committee Reports. They added that the Bill should be 'significantly revised and improved' before returning to Parliament.

Liberal Democrats

- Prior to the publication of the draft Bill, there had been suggestions from senior Lib Dems that they might attempt to block the Bill's progression through the House of Lords.
- The Lib Dems are not supportive of the draft Bill, with Lord Strasburger, a Member of the Joint Committee which is scrutinising the draft Bill providing particularly vocal criticism.

Industry

Apple: Highly critical, with main criticisms centred around effects on encryption of iMessage.

Facebook, Google, Microsoft, Twitter, Yahoo: In a joint statement to the draft Bill Joint Committee, these companies raised concerns over: extraterritorial jurisdiction, encryption, data

retention, judicial authorisation, bulk data collection, transparency and network exploitation. They have called for significant changes to be made to the draft Bill.

ISPA: The ISP trade body has consistently stated that it has concerns with the revised Bill and it needs reform to ensure it is feasible, proportionate and does not harm the UK Internet industry. They agree that a new framework is needed to replace the various outdated laws, but need further clarity on Internet Connection Records, definitions and costs need to be provided.

techUK: The trade association has warned of the Bill potentially having a negative economic impact due to companies losing the trust of users as a result of being subject to broader state surveillance powers.

Think tanks and pressure groups

The Open Rights Group, Liberty and Big Brother Watch have all been highly critical of the draft Bill, with the ORG calling for it to be completely rewritten.

FAQ

Q: What do I need to comply with?

A: In the event that the draft Bill becomes law in its current form, only ITSPA member companies which have been served with a data retention notice will have to implement any changes to remain compliant.

Q: Is encryption being banned?

A: No. Despite much speculation in the media prior to the publication of the Bill and comments from high profile politicians, encryption is not being banned.

Q: Should I reconfigure my network network/business now in case a data retention notice is served on my company?

A: The draft Bill does not include any obligation for a company to do this.

Q: If I am served with a data retention notice, will I be reimbursed for the expense of any new equipment needed to comply with the requirements?

A: Yes, a CSP served with a notice can apply for funding from the Home Office. The Home Office would meet the full cost of any requirements – this is the current policy and the Home Office do not intend to change it at present.

Q: Will more smaller CSPs be served data retention notice if the draft Bill becomes law?

A: The Home Office has stated that they do not intend to serve more data retention notices on smaller CSPs, however there is no guarantee around this current position.