techUK Briefing and Response to New Investigatory Powers Bill
On 1st March, the Home Office published a revised Investigatory Powers Bill, alongside six Codes of Practice and the Government’s response to pre-legislative scrutiny.

In response to three Parliamentary Committees, the Home Office has made a number of changes to the draft Bill, including areas that are directly of interest to techUK members such as encryption, extraterritoriality and definitions of key terms such as “data” and Internet Connection Records (ICRs).

Below is a summary of the key changes as they relate to techUK members and recommendations from the Joint Committee on the draft Investigatory Powers Bill, the Intelligence and Security Committee (ISC) and the Science and Technology Committee.

**Privacy**

**Committee recommendations:** The Intelligence and Security Committee (ISC) called for a section of the Bill to be dedicated to addressing privacy safeguards, for example through an overarching statement on the face of the Bill clearly setting out the universal privacy protections which apply across the full range of investigatory powers.

**Key changes:** Part 1 of the Bill now provides a short overview of the privacy safeguards contained throughout the Bill. This falls short of the recommendation by the ISC, which called for privacy protections to form the backbone of the Bill and not be merely an add-on. The section on privacy in Part 1 reads more like a summary of privacy protections, through the Home Office simply adding the word “privacy” to the sub-heading, rather than an overarching statement that the Government considers the protection of privacy as paramount.

**Definitions**

**Committee recommendations:** The Joint Committee and the Science and Technology Committee both highlighted the concerns within industry as to the overly broad and confusing definitions of terms such as “data”, “internet connection records” (ICRs) and “related communications data”. In seeking to “future-proof” the Bill, the Committees concluded that the Government had created uncertainty within industry that needed addressing.

**Key changes:** The Home Office has made a number of changes to some of the key terms used within the Bill.

For example, the term “related communications data” has been replaced with the term “secondary data”. “Secondary data” is defined as data (that is not content) that can be obtained under a targeted or bulk interception warrant. This is intended to clarify the distinction between this type of data and the narrower class of data available under a communications data authorisation.

The definition of the term “data” has also been changed in line with the Joint Committee’s recommendation. The new definition makes clear that the term “data” in the revised Bill includes “data which is not electronic data and any information (whether or not electronic)”. techUK will be consulting with members over the coming weeks as to whether the new definitions have provided the clarity that the draft Bill lacked.

**Extraterritoriality**
Committee recommendations: The Joint Committee in particular called on the Government to rethink its position on enforcing legislation extraterritorially, referencing Sir Nigel Sheinwald’s important work in paving the way for the creation of a new international framework for intelligence sharing. This was similar to techUK’s recommendation that the Bill must complement rather than conflict with the aim of creating an international legal framework for the lawful acquisition of data by government agencies. The Bill should be viewed as an international piece of legislation, with global implications, and techUK members felt it important that the Bill plot a path to addressing the gaps and conflicts which currently exist between jurisdictions rather than add to this complexity.

Key changes: It seems that little has changed in regards to the concerns that the Intelligence and Security Committee, the Joint Committee and techUK expressed regarding extraterritorial provisions. Although there are greater and more consistent safeguards on proportionality and conflicts of law for overseas providers, extraterritorial provisions that undermine long term objectives still remain.

The Home Office has acknowledged concerns regarding these provisions, but their response in the overarching documents to the Bill has been to reiterate that it is engaging in preliminary discussions with international partners on a new international framework. There has been little information about how these discussions have progressed or how they are “re-doubling their efforts” to create this framework, as recommended by the Joint Committee. Debates in the US have indicated that there is strong Congressional support for an international framework and techUK urge the Government to make this their long term goal. Until then, the Mutual Legal Assistance Treaty (MLAT) process should be established on the face of the Bill as the primary mechanism for investigations involving overseas providers.

Encryption

Committee recommendations: All three parliamentary reports called for further clarity and reassurance on the face of the Bill or within the Codes of Practice that end-to-end encrypted services and products would not be affected by Section 189 notices in the Bill.

Key Changes: The language on encryption has been amended in clauses 217 and 218. Section 189 of the draft Bill proposed that obligations be placed on CSPs “relating to the removal of electronic protection applied by a relevant operator to any communications or data”. This obligation has now been slightly changed in the new Bill, so that obligations now apply “to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data”.

Furthermore, the draft Codes of Practice on Communications Data state that “an obligation placed on a CSP to remove encryption only relates to electronic protections that the company has itself applied to the data, or where those protections have been placed on behalf of that CSP”, such as where a CSP has contracted a third party to apply electronic protections. The Bill has also been revised to make clear that where an obligation is placed on a CSP, which includes the removal of encryption, the technical feasibility and likely cost of complying with those obligations must be taken into account.

The Government maintains that the purpose of this obligation is to ensure that data can be provided in intelligible form, though it is worth pointing out that more detail could have been provided in the Codes of Practice. For example, what is the procedure for when the Home Secretary (on advice of the Technical Advisory Board) and the CSP disagree as to the
technical feasibility of a technical capability notice? This is not clear on the face of the Bill. Furthermore, the decision as to the technical feasibility and likely cost of requiring a CSP to remove electronic protection should not be solely in the hands of the Secretary of State, but should require the involvement of a judicial commissioner.

**Equipment Interference**

**Committee recommendations**: All three Committees stated the risks within provisions in the draft Bill related to equipment interference (EI) powers, particularly in bulk. The Science and Technology Select Committee highlighted the dangers such powers may have on the development of smart technology, whilst the ISC recommended removing bulk equipment powers entirely. For this reason, the Joint Committee called for the Government to introduce detailed risk analyses whenever equipment interference is sanctioned.

**Key changes**: Neither the face of the Bill nor the Codes of Practice acknowledge the dangers inherent within equipment interference provisions. In fact, the key recommendations by the Committees that attempted to safeguard the use of equipment interference have all been ignored and in some instances EI powers have been extended, rather than limited.

For example, despite the draft Codes of Practice on Equipment Interference requiring EI warrants to include “an assessment of any risks to the security or integrity of systems or networks”, this assessment on the face of it seems different to the Joint Committee’s recommendation of a “detailed risk analysis of the possibilities of system damage and collateral intrusion and how such risks will be minimised”.

Furthermore, under provisions in the new Bill police officers will now be able to use EI for “threat to life” situations. The new Bill also provides for the Secretary of State to authorise bulk EI warrants in urgent circumstances. The concerns regarding bulk equipment interference, and the ISC recommendation that bulk equipment interference be removed from the Bill, have therefore been ignored.

There are therefore no provisions within the Bill or Codes of Practice relating to the importance of network integrity and cyber security. Neither is there a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. It is important that EI does not introduce new vulnerabilities into systems and the detailed risk analyses that the Joint Committee recommended would help any assessment of proportionality.

**Internet Connection Records**

**Committee recommendations**: Whilst all three reports recognised an operational need for internet connection records (ICRs), all three reports expressed concerns about the definitions and technical feasibility of retaining such data. The draft Bill contained inconsistent definitions of ICRs that created uncertainty within industry as to their technical feasibility. As techUK has stated in the past, ICRs are not a term that industry has used before and would require a radical departure from normal business practices for industry.

**Key Changes**: Responding to such criticism, the Bill now has a single definition of ICRs that remains consistent throughout the course of the Bill, with references to internet connection records appearing in both the authorisation and retention sections of the Bill.
Furthermore, the draft Communications Data Code of Practice includes a section on ICRs that is consistent with that provided for in the Bill and lists the core information that will be included in an ICR such as: an account reference, a source IP and port address, a destination IP and port address and a time/date.

Tellingly, the Codes of Practice admit that there will be no single set of data that constitutes an internet connection record and that in practice “it will depend on the service and service provider concerned”. This acknowledgement highlights the difficulties that industry will face if required to generate and retain ICRs.

The new Bill has also extended the purposes for which law enforcement can access ICRs to include information about websites that have been accessed that are not related to communications services nor contain illegal material. It seems that rather than addressing the concerns of industry and the public about the scope of powers related to ICRs, the Home Office have responded by extending the powers rather than limiting them.

Gagging Notices

Committee recommendations: The Joint Committee rightly highlighted the importance of allowing CSPs, through a mechanism such as the Technical Advisory Board (TAB), to share details of a retention notice with other CSPs that are under similar notices.

Key changes: CSPs will now be able to discuss their retention obligations with systems suppliers, oversight bodies and other companies that are subject to retention obligations. The Bill has been revised to ensure that CSPs can disclose the existence and contents of such notices with the permission of the Secretary of State.

This is to be welcomed. Transparency is crucial to ensuring that confidence in surveillance practices going forward is maintained – for this reason, more and more companies are now producing transparency reports on the number and nature of requests that they receive for data. The draft Bill, as it was worded, would have prohibited companies from having the same opportunity and also prevented them from communicating with other companies and share technical solutions to retention notices.

Cost retention

Committee recommendations: The Science and Technology Committee and the Joint Committee both received evidence from companies that suggested that the Home Office had underestimated the costs of retaining data, including internet connection records. In light of this, the Science and Technology Committee argued that the Government should rethink its reluctance for including in the Bill an explicit commitment that Government will pay the full costs incurred by compliance in order to reassure industry.

Key changes: On cost retention, the Bill does not go as far as the Science and Technology Committee would have liked and does not put 100% cost recovery on the face of the Bill. The supporting documents, however, reaffirm the Government’s longstanding position of reimbursing 100% of the costs associated with data retention and states that there are “no current plans to change that policy”. Whether this gives industry the reassurance it requires remains to be seen. Government must in the meantime work with industry to improve its estimated costs and ensure that small providers in particular receive the technical and financial support they need to comply with the legislation.

Judicial Commissioners
**Committee recommendations:** Despite concerns from some quarters that the role of the Judicial Commissioners provided for in the draft Bill were merely procedural, the Joint Committee was fairly satisfied with the “double-lock” (Home Secretary and judicial commissioner) authorisation for targeted interception, targeted equipment interference and bulk warrants.

**Key changes:** The Government has amended the Bill at Clause 202 to make it explicit that Judicial Commissioners have the power to initiate investigations and receive complaints directly from industry. This is important and welcome as it will provide a higher level of transparency and oversight than is currently afforded with such powers. It is important to note, however, that the judicial review principles afforded in the Bill do not meet US standards on “probable cause”; which could create difficulties in creating the international framework that is referenced above.

**Bulk Collection**

**Committee recommendations:** All three reports accepted the operational need for bulk collection powers, although the Joint Committee in particular called for the Government to provide fuller justifications for each of the bulk powers afforded in the Bill, acknowledging the need for greater safeguards for bulk powers as they can be highly intrusive.

**Key changes:** The Government has now published an operational case for the bulk powers in the Bill. It is crucial that the operational case is carefully scrutinised by parliamentarians. Unlike in the US, where bulk collection powers under Section 215 of the Patriot Act were debated at length in Congress and scaled back, parliamentarians in the UK have not had a chance to debate such powers in public.

**Post Legislative Scrutiny**

Clause 222 requires the Secretary of State to prepare a report on the operation of the Investigatory Powers Act within six years of the Bill being enacted. This is in anticipation of a Select Committee of either House of Parliament (whether acting alone or jointly) undertaking a review of the powers in the Bill within five years and six months of Royal Assent.

**Other issues**

**Third party data retention**

Chapter 2 of the draft Communications Data Code of Practice includes a clear restriction on third party data retention by CSPs.

**Data Generation**

Chapter 14 of the draft Communications Data Code of Practice confirms that the Bill may require companies to generate new data that they would not already have done for business purposes.

**Consultation**

Six codes of practice have been published alongside the bill, including ones on Equipment Interference and ICRs. There will be a full consultation period on these Codes once the Bill received Royal Assent.

**Next Steps**

This is a complex Bill, with significance for all of us. Parliamentarians must have time necessary to subject it to the “maximum parliamentary scrutiny” the Home Office has promised. It’s
important the Bill is not rushed through Parliament if we’re to achieve the world leading legislation Government has committed to delivering.

We will be working with members to fully understand the implications for their businesses and the industry as a whole.