INVESTIGATORY POWERS BILL: OBLIGATIONS ON COMMUNICATIONS SERVICE PROVIDERS (CSPs)

The use of investigatory powers relies heavily on the cooperation of communications service providers (CSPs) in the UK and overseas. The assistance of CSPs is frequently required to obtain communications data relating to a person's use of a particular service or to intercept communications sent by that service. The assistance of CSPs may also be necessary in order to gain direct access to a suspect's device by using equipment interference powers.

CSP Obligations

The obligations on CSPs to provide assistance in relation to the use of investigatory powers are spread across a number of different laws:

- DRIPA requires CSPs to retain certain types of communications data; additional retention requirements are provided under the CTSA.

- RIPA requires CSPs to provide communications data when served with a notice, to assist in giving effect to interception warrants, and to maintain permanent interception capabilities, including maintaining the ability to remove any encryption applied by the CSP to whom the notice relates.

- The Telecommunications Act 1984 requires CSPs to comply with directions issued by the Secretary of State in the interests of national security; this includes the acquisition of bulk communications data.

The Bill will bring together these obligations in a single, comprehensive piece of legislation. It also provides an explicit obligation on CSPs to assist in giving effect to equipment interference warrants. Only those agencies that are able to apply for an interception warrant will have the ability to serve such warrants, which must be authorised by the Secretary of State and approved by a Judicial Commissioner. The Bill does not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA.

The Bill provides for the Secretary of State to require CSPs to maintain technical capabilities relating to the powers under the Bill. The purpose of maintaining a technical capability is to ensure that, when a warrant is served, companies can give effect to it securely and quickly. This provision will replace the current obligation to maintain a permanent interception capability and will provide a clear basis in law for CSPs to maintain infrastructure and facilities to give effect to interception and other warrants.

Before giving a technical capability notice, the Secretary of State must consult the CSP to whom the notice is to be given and must take into account the effect of the notice on the provider, with specific consideration of the cost and technical feasibility of any obligations relating to the removal of encryption. The Secretary of State can then give a notice only if he or she considers that the requirements imposed by a notice are

necessary and proportionate to what is sought to be achieved, and the decision to give a notice has been approved by a Judicial Commissioner.

CSPs may also be required to provide assistance to law enforcement and the security and intelligence agencies in the interests of national security through a national security notice given by the Secretary of State. This provision will replace the general power of direction under the Telecommunications Act 1984. The new power will be used very sparingly and only if the Secretary of State and a Judicial Commissioner are satisfied that the notice is necessary and proportionate. The power is subject to strict safeguards which prevent it from being used for the primary purpose of authorising or requiring a CSP to disclose communications or communications data or acquiring data. In any circumstance where a notice would involve the acquisition of communications or data as its main aim, an additional warrant or authorisation provided for elsewhere in the Bill or in other relevant statutes would always be required. More detail on the use of national security notices has been provided in the draft National Security Notice Code of Practice.

The ability for CSPs to request a review of their obligations will be strengthened through the Bill. The Bill provides for the continued existence of the Technical Advisory Board (TAB), which comprises industry and agency experts and provides advice to the Secretary of State on the cost and technical feasibility of implementing a particular obligation. In future, CSPs will be able to request a review of the obligations imposed on them in technical capability notices, national security notices, or data retention notices. The Secretary of State will be obliged to take advice from the TAB and the Investigatory Powers Commissioner before deciding the review. The circumstances in which reviews will be permitted will be broadened to take account of CSPs' changes to services and infrastructure and when a notice is varied.

Overseas Companies

Interception and communications data powers rely on the support of overseas companies. The existing obligation in RIPA to comply with interception warrants (including for bulk interception) and communications data acquisition notices was clarified in 2014 through DRIPA. Other investigatory powers (such as data retention) may rely on the support of overseas companies.

The Bill places the same obligations on all companies providing services to the UK or in control of communications systems in the UK. However, the Bill only provides for those obligations to be enforced through the courts against overseas companies in respect of targeted communications data acquisition and (targeted and bulk) interception powers. The Bill will include explicit provision to require the Secretary of State to take account of any potential conflict of laws that overseas companies may face.