# INVESTIGATORY POWERS BILL: PRIVACY

The Investigatory Powers Bill will protect both privacy and security. Part 1 of the Bill provides an overview of the privacy safeguards contained throughout the Bill. The Bill and the accompanying Codes of Practice make clear the strong privacy safeguards that apply to all of the powers in the Bill, in particular:

- **Privacy:** the privacy clause in the first part of the Bill makes clear that protections around privacy are at the heart of the Bill. It sets out the privacy considerations that must be taken into account before issuing any warrant, authorisation or notice provided for in the Bill. It mandates that a public authority must consider: whether what is sought to be achieved by the warrant, notice or authorisation could be achieved by other less intrusive means; the public interest in the integrity and security of telecommunication systems and any other aspect of public interest in the protection of privacy. The robust safeguards that apply to the use of every investigatory power contained in the Bill are set out in further detail in each Part.

- **Transparency:** the Bill makes more explicit the powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. Some powers will remain outside of the Bill. For example, in line with the recommendation made by David Anderson QC, the police will retain the ability to use overt search and seizure powers to obtain communications that have been stored on a device or a server, such as emails stored on a web-based server. The Bill also imposes requirements on the Investigatory Powers Commissioner to report to the public and to Parliament precisely how the powers in the Bill have been exercised.

- **Authorisation:** The Bill overhauls the way the most sensitive powers available to law enforcement and the security and intelligence agencies are authorised. Under the Bill, warrants will be subject to a new 'double lock', so that they must be approved by a Judicial Commissioner before they can be issued by the Secretary of State. The Judicial Commissioner will review the decision of the Secretary of State applying judicial review principles. This will preserve democratic accountability and introduce a new element of judicial independence into the authorisation process. This powerful new safeguard was endorsed by the Joint Committee convened to scrutinise the draft Bill. In response to concerns expressed during Commons Committee Stage, the Government introduced an amendment to make clear that when carrying out a review of a decision to issue a warrant, the Judicial Commissioner must do so with a sufficient degree of care as to ensure that the Commissioner complies with his or her duties under clause 2 (general duties in relation to privacy).

- **Oversight:** The Bill creates a world-leading oversight regime, bringing together three existing commissioners and providing new powers and resources to an independent Investigatory Powers Commissioner (IPC). The Commissioner will hold, or have held, high judicial office and will oversee the use of the powers in the Bill by public authorities. The revised Bill strengthens the office of the IPC further. Where the IPC in the course of his or her investigations determines that a person

has been the subject of a serious error, the IPC will have the ability to notify the individual concerned.

- **Limited powers:** the Bill strictly limits the circumstances in which the powers it provides for can be used. In line with the recommendation made by the Intelligence and Security Committee in its 2015 Privacy and Security report, the revised Bill and the accompanying Codes of Practice make clear:

    - The purposes for which each of the powers in the Bill may be used. Those powers that can be used to access the content of communications or other private documents, such as interception and equipment interference, may only be used for a very limited number of statutory purposes.

    - The overarching human rights obligations which constrain the use of the powers in the Bill. This includes statutory obligations elsewhere in domestic and international law.

    - Whether each of the powers in the Bill must be used in a targeted way or provides for the acquisition of data in bulk. The Bill also makes clear that a Secretary of State and a Judicial Commissioner (the 'double lock') must approve the purposes for which data obtained in bulk can be examined.

    - The authorisation procedures that must be followed, including the review, inspection and oversight regime. This includes the introduction of a new 'double lock' for all warrants in the Bill.

    - Specific safeguards for certain sensitive professions or categories of information. This includes additional protections in the Bill and the statutory Codes of Practice for lawyers, Parliamentarians and journalists.

    - Safeguards and obligations in respect of retention, storage and destruction of data. In particular, the Bill and the accompanying materials make clear the security obligations relating to retained data.

    - Safeguards relating to sharing of material obtained under the powers in the Bill. These are set out on the face of the Bill and the accompanying Codes of Practice.

- **Penalties for misuse:** the Bill sits alongside existing legislation such as the Computer Misuse Act 1990 to make clear the circumstances in which it is an offence to obtain communications or communications data without a lawful authorisation. Part 1 of the Bill sets out relevant offences in other legislation.