News story: Safeguards governing investigatory powers come into effect

From today, warrants permitting the use of the most intrusive investigatory powers will require the approval of a judge.

This marks the final step needed to implement the stringent 'judicial double-lock' safeguard created by the landmark Investigatory Powers Act 2016. The safeguard requires judicial approval in addition to existing authorisations, before certain powers can be used.

At midnight, the government commenced the equipment interference provision for law enforcement agencies and wider public authorities – the final provision to require a warrant subject to the double-lock.

The Investigatory Powers Act overhauls the way in which investigatory powers are authorised and overseen.

In addition to the double-lock, it created the role of the Investigatory Powers Commissioner to oversee the intelligence agencies, police and other public authorities' use of investigatory powers.

Security Minister Ben Wallace said:

> The terrorist attacks last year and the reckless use of a nerve agent in the UK earlier this year were stark reminders of the real and significant national security threats this country faces. We are also aware that serious and organised crime is costing this country at least £37 billion each year, let alone the devastating human impact.
>
> It is essential that our law enforcement, security and intelligence agencies and wider public authorities have the powers they need to investigate and disrupt the most dangerous criminals and national security threats.
>
> The Investigatory Powers Act is world-leading legislation, providing strict safeguards and unprecedented oversight. The double-lock ensures that these vital tools are used in a way that is both necessary and proportionate.

The Investigatory Powers Act brought together and updated existing powers that are available to law enforcement and the security and intelligence agencies. It created one new power allowing access to internet connection records, vital in confronting serious criminals, terrorists and hostile state activity in a digital age.

Separately, the government will introduce independent judicial authorisation

of the acquisition and retention of communications data. The legislation is already in place to enable this and the changes will come into force next year.

Powers subject to judicial authorisation

Equipment interference (EI) allows authorised bodies, including law enforcement and the intelligence services to interfere with equipment, such as computers and smartphones, to obtain communications, equipment data or other information from the device. Where necessary and proportionate, this power is used to gain valuable intelligence in national security and serious and organised crime investigations and to help gather evidence for use in criminal prosecutions.

Interception is obtaining the content of a communication – such as a telephone call, email or social media message – during its transmission or while stored on a telecommunications system. This power is a vital tool that helps law enforcement and the security and intelligence agencies detect and prevent serious and organised crime, and to protect national security.

Bulk personal datasets (BPD) are sets of personal information about many people held on electronic systems such as the electoral roll, the majority of whom will not be of any specific interest to the security and intelligence agencies. Their retention and examination by the security and intelligence agencies are essential in helping to identify subjects of interest or individuals who surface during an investigation, to establish links between individuals and groups and to understand a subject's behaviour and connections better to quickly exclude the innocent. This enables the agencies to focus their attention on specific individuals or organisations that threaten our national security.

Bulk powers for interception, communications data acquisition and equipment interference provide the ability to collect large volumes of data, which can be selected for further examination, and is crucial in enabling the security and intelligence agencies to investigate known, high-priority threats and to identify emerging threats from individuals previously not known to them. Terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Access to bulk data enables the security and intelligence agencies to obtain intelligence on overseas subjects of interest, identify threats here in the UK and establish and investigate link between known subjects of interest at pace.

Communications data (acquisition and retention) provides law enforcement, the agencies and other specified public authorities access to information about a communication – the who, where, when, how and with whom of a communication but not what is written or said. This information is acquired from communications service providers (CSPs) who may also be required to retain the communications data. Requests for communications data are made to identify the location of missing people or to establish links (through call records) between a suspect and a victim. It can be the only way to identify offenders, particularly where the offences have been committed online, such

as fraud and child sexual exploitation.