Investigatory Powers Bill

Key points

- Equipment interference (EI), sometimes referred to as computer network exploitation, is the power to obtain a variety of data from equipment. This includes traditional computers or computer-like devices such as tablets, smart phones, cables, wires and static storage devices. EI can be carried out either remotely or by physically interacting with equipment.
- The Bill creates clearer, robust safeguards to the regime, making sure that equipment interference is only used when necessary and proportionate for a legitimate purpose.
- A 'double-lock' authorisation procedure will be in place requiring warrants issued by a Secretary of State or a Chief Constable (or equivalent), to be approved by a Judicial Commissioner before coming into force.
- Law enforcement agencies able to apply for an EI warrant are limited to UK police forces, the NCA, HMRC, the Ministry of Defence police, Royal Military Police, Royal Navy Police and the Royal Air Force Police.
- Equipment interference capabilities have made a vital contribution to counter the increased threat to the UK from Islamist terrorism and have also enabled the disruption of paedophile-related crime. Without EI the ability of the security and intelligence agencies, armed forces and law enforcement agencies to protect the public from terrorism, cyber-attack, serious crime, including child sexual exploitation, and a range of other threats would be seriously degraded.

Background

- Equipment interference allows the security and intelligence agencies, armed forces and law enforcement agencies, to interfere with equipment for the purpose of obtaining electronic data from the equipment.
- EI operations vary in complexity. A straightforward example is the use of the login credentials of a target to gain access to the data held on a computer. More sophisticated EI operations may involve remotely installing a piece of software on to a device. The software could be delivered in a number of ways and then be used to obtain the necessary intelligence.
- The use of this capability by the security and intelligence agencies was avowed in February 2015 through a draft Equipment Interference Code of Practice.

Key facts

- In order to keep pace with changing technology it has been necessary for agencies to develop techniques to enable them to gain access to computers, devices and other web-based activities to gather evidence or intelligence.
- GCHQ conducts EI operations with a foreign focus to protect the UK and its interests. During 2013 around 20% of GCHQ's intelligence reports contained information that derived from EI operations against a target's computer or network.
- MI5 has relied on EI in the overwhelming majority of high priority investigations over the past 12 months. It has been instrumental in disrupting credible threats to life, including against UK citizens.

Key Quotes

"Changes in the technology that people are using to communicate are making it harder for the Agencies to maintain the capability to intercept the communications of terrorists. Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced."
Andrew Parker, Terrorism, Technology and Accountability (RUSI, 8 Jan 2015)

"This task is, of course, becoming more complicated. The evolution of the internet and modern forms of communication provide those who would do us harm with new options; they provide those who would protect us – the police, the security and intelligence agencies, the National Crime Agency and others – with new challenges."
Home Secretary, Defence and Security Lecture (Mansion House, 24 June 2014)

Investigatory Powers Bill

Why do we need it?

- Equipment Interference is used to secure valuable intelligence to enable the Government to protect the UK from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality. It also helps law enforcement agencies to protect the most vulnerable members of society.
- EI operations may enable security and intelligence agencies, or law enforcement agencies, to obtain communications and other data of individuals who are engaged in activities that are criminal or harmful to national security that would otherwise be unobtainable. For instance, when a key piece of information encrypted in transmission, so cannot be intercepted.
- EI may in some cases be the only way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country.

Who can do it? Under what authority?

- The security and intelligence agencies, armed forces and law enforcement agencies can apply for an Equipment Interference Warrant.
- Law enforcement agencies' equipment interference authorisations are issued by a Chief Constable (or equivalent) and approved by an independent Judicial Commissioner. A warrant can be applied for the prevention and detection of serious crime.
- The armed forces' warrants are issued by a Secretary of State and approved by an independent Judicial Commissioner. A warrant can be applied for in the interests of national security.
- Security and intelligence agencies' warrants are issued by a Secretary of State and approved by an independent Judicial Commissioner. A warrant can be applied for in the interests of national security, preventing and detecting serious crime, and in the interests of economic well-being (where they are also relevant to the interests of national security).
- Equipment interference warrants last for six months.
- Material derived from equipment interference may be used in evidence.

What are the safeguards?

- Equipment interference for the purposes of acquiring communications, equipment data or private information by security and intelligence agencies, armed forces or law enforcement agencies will require a warrant.
- A 'double-lock' authorisation procedure will be in place requiring warrants issued by a Secretary of State or a Chief Constable (or equivalent), to be approved by Judicial Commissioner before coming into force.
- Warrants will need to make clear the necessity and proportionality of the action being taken.
- The Investigatory Powers Commission will oversee the exercise of equipment interference, including inspection and audit of handling arrangements.
- A statutory code of practice will set out the handling, destruction, retention arrangements and safeguards for material acquired.
- Any individual who thinks that surveillance powers have been used against them unlawfully can make a complaint to the Investigatory Powers Tribunal.

What is new?

- Equipment interference is not a new power – it is already provided for under Section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. A Code of Practice on equipment interference sets out procedures and safeguards relating to its use by the SIA.
- The equipment interference power in the Investigatory Powers Bill will set out a clear statutory framework for equipment interference for the purpose of obtaining data. The new legislation will update the current legal framework for authorising EI operations, ensuring that it is modern, transparent and fit for purpose.
- The armed forces will also be able to apply for targeted equipment interference warrants. They have been able to carry out this activity previously with assistance from GCHQ; this Bill gives them the power to authorise this activity independently as required to support military operations overseas.
- The Bill will create a new power to require the assistance of CSPs where necessary, to give effect to equipment interference warrants, bringing EI into line with interception and providing a clear oversight and appeals framework for this process.