Home Office

Investigatory Powers Act 2016

Consultation: Codes of Practice

February 2017

Ministerial Foreword

The Investigatory Powers Act concluded its Parliamentary passage on 16 November 2016 and received Royal Assent on 29 November 2016. The Act does three key things:

- First, it brings together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It makes these powers – and the safeguards that apply to them – clear and understandable.

- Second, the Act radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for the most intrusive powers, including interception and all of the bulk capabilities, so that warrants cannot be issued until the decision to do so has been approved by a Judicial Commissioner. And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.

- Third, it ensures powers are fit for the digital age. The Act makes a new provision for the retention of internet connection records in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate.

It is essential our law enforcement, security and intelligence services have the powers they need to keep people safe. The internet presents ever-evolving opportunities for terrorists, criminals and paedophiles, and we must ensure that we have the capabilities to confront this challenge. There must be no guaranteed safe spaces online in which they are allowed to communicate beyond the reach of law. But it is also right that these powers are subject to strict safeguards and rigorous oversight.

The Investigatory Powers Act provides world-leading transparency and privacy protection. It received unprecedented and exceptional scrutiny in Parliament and was passed with cross-party support. There should be no doubt about the necessity of the powers that it contains or the strength of the safeguards that it includes.

The draft Codes of Practice published for public consultation set out the processes and safeguards governing the use of investigatory powers. They give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with this important legislation.

All responses will be welcomed and carefully considered.

Ben Wallace MP

Minister of State for Security

Contents

Scope of the consultation

Topic of this consultation:	This consultation is on five draft codes of practice under the Investigatory Powers Act 2016 (IP Act): • Interception of communications • Equipment interference • Bulk communications data acquisition • Bulk personal datasets • National Security Notices
Scope of this consultation:	This consultation seeks representations on the draft codes of practice.
Geographical scope:	UK-wide

Basic Information

To:	Representations are welcomed from communications service providers, public authorities that have powers under the IP Act, as well as professional bodies, interest groups and the wider public.
Duration:	6 weeks, closing on 6 April 2017
Enquiries and responses:	*investigatorypowers@homeoffice.gsi.gov.uk* Please indicate in your response whether you are content for it to be published, with or without attributing it to you/your organisation.
After the consultation:	Following the consultation period, responses will be analysed and the draft codes revised as necessary. They will then be laid before Parliament for approval.

Background

Getting to this stage:	The Government consulted widely before producing the draft Investigatory Powers Bill which was then published for pre-legislative scrutiny. The draft Bill responded to three independent reports, which all agreed a new law was needed. A Joint Committee of both Houses of Parliament was established to study our proposals, and two further Parliamentary committees conducted parallel scrutiny. We carefully considered the committees' recommendations and the majority of these were addressed in our revised Bill and the further material that we published alongside it, including drafts of the codes of practice to be made under the Investigatory Powers Act. We published updated versions of the draft codes in autumn 2016 to reflect changes made to the Bill and commitments made by the Government during the Bill's passage up to that point. The drafts of the codes published for this consultation reflect further changes in the final Act, and continued consultation with the bodies affected and other interested groups. In preparing these drafts we have consulted extensively with communication service providers, the law enforcement and intelligence community and the three existing Commissioners who oversee and monitor aspects of the legislation (Office of the Interception of Communications Commissioner, Office of the Surveillance Commissioners, and Intelligence Services Commissioner). We have also engaged with representatives of legal bodies, journalists' groups, civil liberties organisations, and both Government and industry technical experts.

What are codes of practice?

These codes set out the processes and safeguards governing the use of investigatory powers by public authorities including the police and security and intelligence agencies. They give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with this important legislation.

These codes are primarily intended to guide those public authorities which are able to exercise powers under the Investigatory Powers Act 2016. The codes will also be informative to staff of communications service providers which may be served with warrants or given notices under these Acts.

Once issued, the codes of practice have statutory force and individuals exercising functions to which the codes relate must have regard to them. They are admissible in evidence in criminal and civil proceedings and may be taken into account by any court, tribunal or supervisory authority when determining a question arising in connection with those functions.

Each code includes an introductory chapter to explain its individual scope and the powers it relates to.

Why are we consulting?

Under the Investigatory Powers Act 2016, the Secretary of State is required to issue codes of practice about the exercise of functions under the Act. Schedule 7 of the Act sets out further requirements which the codes must satisfy. Prior to issuing the codes, the Secretary of State must prepare and publish draft codes. This consultation fulfils that requirement.

Following the consultation, the Secretary of State must consider any representations made about the drafts and Parliament must approve the final codes before they can come into effect.

Codes under the Investigatory Powers Act 2016

The Investigatory Powers Act 2016 governs the powers available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. The five draft codes of practice relate to the powers described below. All of these powers are subject to strict safeguards. The most intrusive powers are subject to a 'double lock', whereby warrants must be approved by a Judicial Commissioner before they are issued.

Interception of communications

Interception is the power to obtain a communication in the course of its transmission.

Targeted interception warrants authorise the interception of communications or the obtaining of secondary data from communications.

Bulk interception is used by the security and intelligence agencies to obtain overseas-related communications (or secondary data) in large volumes in order to find intelligence on known threats and to identify new ones. This data is subject to very stringent controls to filter the material obtained and select a fraction of it for examination. This data may not be available by other means.

Equipment Interference

Equipment interference means interfering with equipment in order to obtain communications, equipment data or other information. The equipment in question could include traditional computers or computer-like devices such as tablets, smart phones, cables, wires and static storage devices. Equipment interference can be carried out either remotely or by physically interacting with equipment.

Bulk equipment interference describes a set of techniques to obtain information from devices that is necessary for the identification of subjects of interest who pose a threat to the UK's national security. Bulk equipment interference will provide access to intelligence currently available through bulk interception, but which may not be available in future. As with bulk interception, this data may not be available by other means and must be foreign-focused.

Bulk communications data acquisition

Communications data includes data about communications but does not include the content of communications, and is typically required by communications service providers to process and/or transmit the communications themselves. It might include the date and time of a phone call or the sender and recipient of an email, but does not include the words spoken or text sent.

Bulk communications data acquisition is the collection of this type of data in large volumes by the security and intelligence agencies.

Access to this data is essential to enable the identification of communications data that relates to subjects of interest and to subsequently piece together the links between them. Where a security and intelligence agency has only a fragment of intelligence about a threat or an individual, communications data obtained in bulk may be the only way of identifying a subject of interest. Identifying the links between individuals or groups can also help the agencies to determine where they might request a warrant for more intrusive acquisition of data, such as interception.

An additional code of practice covering the obtaining and retention of communications data (under Parts 3 and 4 of the Investigatory Powers Act 2016) will be published for consultation in due course.

Bulk personal datasets

A bulk personal dataset is a dataset containing information about a number of individuals, most of whom are not of interest to the security and intelligence agencies. Analysis of bulk personal datasets is an essential way for the security and intelligence agencies to focus their efforts on individuals who threaten our national security.

Bulk personal datasets can help to eliminate the innocent from suspicion without using more intrusive investigative techniques, establish links between subjects of interest or better understand a subject of interest's behaviour, and verify information obtained through other sources (for example agents) during the course of an investigation or intelligence operation.

A list of people who have a passport is a good example of such a dataset – it includes personal information about a large number of individuals, the majority of which will relate to people who are not of security or intelligence interest.

National Security Notices

The Secretary of State can give a national security notice to a telecommunications operator requiring them to take steps in the interests of national security. They are a critical tool in protecting our national security.

The type of support that may be required includes the provision of services or facilities which would help the intelligence agencies in safeguarding the security of their personnel and operations, or in providing assistance with an emergency.

A notice may typically require a telecommunications operator to provide services to support secure communications by the security and intelligence agencies, for example by arranging for a communication to travel via a particular route in order to improve security. They may additionally cover the confidential provision of services to the agencies within the telecommunications operator, such as by maintaining a pool of trusted staff for management and maintenance of sensitive communications services.

This publication is available at:
http://www.gov.uk/government/collections/investigatory-powers-bill

Any enquiries regarding this publication should be sent to us at *investigatorypowers@homeoffice.gsi.gov.uk*.