Home Office

Investigatory Powers Act 2016

Consultation: Revised Interception of Communications Code of Practice

July 2022

Ministerial Foreword

The Investigatory Powers Act 2016 provides a regulatory framework for the use of a number of covert investigatory powers, to ensure that the powers are used by public authorities in a lawful way that is compliant with the UK's obligations under the European Convention on Human Rights. This involves ensuring that the use of the powers is always closely supervised and constantly reassessed to ensure that what is being done is justified.

The IPA incorporated a number of important safeguards to guard against arbitrary or excessive use of the powers, including a strict authorisation framework and provision for independent oversight and review of the use of the powers.

Section 4 of the IPA states that a person intercepts a communication in the course of its transmission by means of a telecommunication system if they perform a relevant act in relation to the system and the effect of that act is to make any content of the communication available at a relevant time to a person who is not the sender or intended recipient of the communication.

The use of interception is key to protecting national security and fighting serious crime. It allows investigators to gain an insight into the criminal and terrorist organisations they are targeting. For decades, interception has played a crucial role in preventing, and securing prosecutions for, serious crimes including terrorism, drugs and firearms offences, as well as child sexual exploitation and abuse. This has included helping to identify and disrupt many of the terrorist plots that have been prevented. The IPA is supplemented by the Interception Code of Practice which provides detailed, comprehensive guidance and best practice on the use of Interception. It is intended to guide law enforcement agencies, the security and intelligence agencies and other public authorities who exercise such powers. It sets out additional safeguards as to how the powers already in primary legislation should be exercised and the duties performed. The Interception Code of Practice was issued in 2018. The draft version on which we are consulting has been revised and updated to reflect HMG's position on Cloud-service providers and the enterprise services they provide to customers, and the circumstances in which an Intercepting Authority should serve a warrant on either the Cloud-service provider or the enterprise customer. These changes will bring much needed clarity for US Communications Service Provider (CSPs) and UK Telecommunications Operators (TOs) who are impacted by enterprise service issues.

All responses will be welcomed and carefully considered.

Rt Hon Priti Patel MP

Home Secretary

Contents

Scope of the consultation

Topic of this consultation:	This consultation is on proposed changes to the Interception Code of Practice (CoP), to ensure the CoP is clear on the circumstances in which an Intercepting Authority should serve a warrant on either the Cloud-service provider or the enterprise customer.
Scope of this consultation:	This consultation seeks representations on the draft revised Code of Practice.
Geographical scope:	UK-wide

Basic Information

To:	Representations are welcomed from public authorities that have powers under the IPA, as well as professional bodies, interest groups and the wider public.
Duration:	8 weeks
Enquiries and responses:	Please send any enquiries and responses to: InterceptionCodeOfPractice@homeoffice.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 Code revised as necessary. It will then be laid before Parliament for approval.

Background

Getting to this stage:	In preparing this draft we have engaged with public bodies that utilise interception including the law enforcement community. We are also seeking input from the independent Investigatory Powers Commissioner's Office which oversees and monitors the operation of the legislation.

What is the Code of Practice?

The Code is primarily intended to guide those public authorities that exercise powers and perform duties under the Investigatory Powers Act 2016.

The Code sets out the processes and safeguards governing the use of interception by public authorities, including the police and security and intelligence agencies. It gives detail on how the powers should be exercised and duties performed, including examples of best practice. It is intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with the legislation.

A Code of Practice issued under the IPA has statutory force and individuals exercising powers and performing duties to which the Code relates must have regard to it. The Code is 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 powers and duties.

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 powers and performance of duties under the Act.

Prior to issuing any Code, the Secretary of State must prepare and publish a draft of it. The Secretary of State must also consider any representations made about the draft revised Code and may modify the draft accordingly.

This consultation fulfils that requirement. The revised code comes into force in accordance with regulations made by the Secretary of State and the statutory instrument containing such regulations must be laid before Parliament for approval.

Proposed changes:

The change is to make the following addition to the Interception Code of Practice, set out below:

Cloud-service providers make cloud-based services available to enterprises. By "enterprises", we mean companies, academic institutions, non-profit organisations, government agencies, and similar entities that pay cloud-service providers to store and/or

process their organisation's electronic communications and other records. When a cloud-service provider is providing such services to an enterprise, the enterprise is responsible for providing accounts to their users and determining the reasons for which data is retained and processed. An intercepting authority seeking targeted interception of data belonging to the enterprise can often obtain the same data from both the cloud service provider and the enterprise. Although the Act allows the intercepting authority to serve the warrant on either the cloud-service provider or the enterprise, the intercepting authority should, where it is reasonable to do so, always serve a copy of the warrant on the enterprise rather than the cloud service provider.

Exceptions to this general rule exist. Situations will arise where it is unreasonable to serve the warrant on the enterprise itself including where it is not technically feasible for the enterprise to give effect to the warrant. In those situations, the intercepting authority may serve the warrant on the cloud-service provider.

For example, it would be unreasonable to serve a warrant on the enterprise itself when the enterprise is wholly devoted to criminal conduct, or where the criminal activity involves senior leadership within the enterprise customer. In those situations, service of the warrant upon anyone within the enterprise customer may create an undue risk to operational security (e.g., there is no appropriate point of contact within the enterprise and there are reasonable grounds to believe that serving the warrant would result in the destruction of data which is the subject of the warrant, or serving the warrant would result in the person under investigation becoming aware of the investigation and likely to interfere with it).

Cloud Service Provider A (a telecommunications operator) provides a telecommunications service (a hosted email platform) to Company B, where Company B is responsible for providing use of this platform to its employees. An intercepting authority is investigating Person C, an employee of Company B suspected of using Company B's email platform to facilitate serious criminal activity. The intercepting authority determines that both Cloud Service Provider A and Company B are technically capable of giving effect to the targeted interception warrant. Because Company B or its senior leadership is not believed to be involved in Person C's criminal activity, nor is it assessed that having Company B give effect to the warrant would unduly compromise operational security, the intercepting authority serves a copy of the targeted interception warrant on Company B. In situations where the enterprise's lack of technical capability is the only reason for serving the targeted interception warrant on the cloud-service provider, the cloud-service provider should be permitted to consult with the enterprise for purposes of providing technical assistance that would allow the enterprise to give effect to the targeted interception warrant.

Even where Person C's criminal activity includes others within the company, e.g. Persons D, E, and F, who are not within Company B's senior leadership, an intercepting authority should still serve the warrant on Company B rather than Cloud Service Provider A as long as doing so would not create an undue risk to operational security

This publication is available at www.gov.uk/government/publications

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