Home Office

Regulation of Investigatory Powers Act 2000

Consultation: Equipment Interference and Interception of Communications Codes of Practice

6 February 2015

Ministerial Foreword

The abilities to read or listen to a suspect's communications or to interfere with his or her computer equipment are among the most important, sensitive, and closely scrutinised powers available to the state. As the threat to the UK from terrorism, espionage and organised crime has diversified, these powers have become more important. Those who mean us harm use internet-based communications to plan, direct and – increasingly – execute their plots. Terrorists, paedophiles and serious criminals are increasingly sophisticated in their use of technology and they are going further in their efforts to evade detection. It is vital that the police and their partners in the Security and Intelligence Agencies are able to stop them.

There are limits on what can be said in public about this work. But it is imperative that the Government is as open as it can be about these capabilities and how they are used. The public and Parliament needs to have confidence that there is a robust statutory framework for the use of such intrusive investigative powers and that there is a strong system of safeguards in place.

The revised and updated draft Interception of Communications Code of Practice published today provides more information than ever on the safeguards that apply to the security and law enforcement agencies' work to identify and disrupt threats. And it provides further detail on the protections afforded to the most sensitive communications (such as those between lawyer and client) that may be intercepted.

The new draft Equipment Interference Code of Practice details the safeguards applied to different investigative techniques, including the use of computer network exploitation, to identify, track and disrupt the most sophisticated targets. It makes clear the role of the Secretary of State in authorising the use of such intrusive techniques only where it is necessary and proportionate to do so. This new draft Code reflects the approach in the existing and published guidance in the Covert Surveillance and Property Interference Revised Code of Practice.

In order to continue to keep us safe, the Security and Intelligence Agencies need the full range of investigatory tools at their disposal. But the public needs to know that these powers are used appropriately and are subject to stringent oversight.

We look forward to receiving your responses.

James Brokenshire MP

Minister of State for Immigration and Security

Why are we consulting?

This consultation contains proposals to update the Interception of Communications Code of Practice and to publish a new Equipment Interference Code of Practice. The Regulation of Investigatory Powers Act 2000 (RIPA) requires the Secretary of State to prepare and publish a draft of these Codes and to consider any representations made about those drafts. This consultation fulfils that requirement.

Scope of the consultation

Topic of this consultation:	This consultation is on the draft Interception of Communications Code of Practice and the draft Equipment Interference Code of Practice.
Scope of this consultation:	This consultation seeks representations on the draft Codes of Practice.
Geographical scope:	UK wide.

Basic Information

To:	Representations are invited from Parliament, professional bodies, interest groups and the wider public.
Duration:	6 weeks, closing on 20 March 2015.
Enquiries and responses:	*Enquiries and responses should be sent to RIPA@homeoffice.x.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 accordingly. They will then be laid before Parliament for approval.

Background

Getting to this stage:	We consulted the law enforcement and intelligence community, the Interception of Communications Commissioner (who oversees the operation of Part 1 of the Regulation of Investigatory Powers Act 2000) and the Intelligence Services Commissioner (who oversees the operation of sections 5 to 7 of the Intelligence Services Act 1994).

Introduction

The ability to intercept the communications of those who mean us harm is a vital tool in the fight against terrorism and serious crime. Since 2010, the majority of the MI5's top priority UK counter-terrorism investigations have used intercept capabilities in some form to identify, understand or disrupt plots seeking to harm the UK and its citizens.

Interception is among the most intrusive powers available to law enforcement and the security agencies. For that reason it is subject to strict safeguards in the Regulation of Investigatory Powers Act 2000 (RIPA). Interception warrants are issued and renewed by the Secretary of State, for a small number of agencies and for a limited range of purposes. RIPA also provides for independent oversight by the Interception of Communications Commissioner and an impartial route of redress, through the Investigatory Powers Tribunal.

Increasingly, terrorists and serious criminals are using sophisticated techniques to communicate covertly and evade detection. That requires the Security and Intelligence Agencies in particular to make use of new and innovative capabilities to identify and disrupt them. The Security Services Act 1989 and the Intelligence Services Act 1994 (ISA) provide the legislative basis for the Security and Intelligence Agencies (SIA) - the Security Service (MI5), the Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ) - to interfere with computers and communications devices. Warrants may only be issued by the Secretary of State where they consider the activities to be authorised are necessary and proportionate. The use of the powers is subject to independent oversight by the Intelligence Services Commissioner.

Interception of Communications

This Code of Practice regulates the powers and duties conferred or imposed under Chapter 1 of Part 1 of RIPA, which provides for the interception of communications. It also provides guidance on the procedures that must be followed before interception under a warrant may take place.

The extant interception Code was brought into force in 2002.

This Government is committed to making publicly available significantly more information about the safeguards that underpin the interception of external communications under section 8(4) of RIPA. These are not new safeguards – the Security and Intelligence Agencies have always had robust internal arrangements, which are overseen by the Interception of Communications Commissioner – but we are now able to put more detail into the public domain than we ever have before.

The key changes reflected in the revised draft Code of Practice are:

- Additional information on the safeguards that exist for the interception and handling of external communications under section 8(4) RIPA.

- Further information around the protections afforded to legally privileged material and other confidential material. This makes explicit the robust safeguards that ensure such communications are not misused.

- Minor changes to reflect the following provisions in the Data Retention and Investigatory Powers Act 2014 (DRIPA):

    - Extra-territoriality. The Code provides guidance on service of warrants and notices on communication service providers outside the UK.

    - Telecommunication services. The Code reflects the clarification of the existing definition of "telecommunications service" in RIPA which makes clear that internet based services are included.

- Changes to reflect developments in the law since 2002, including:

    - Amendments to reflect the introduction of the Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations, which came into force in June 2011 and which provided for a new offence of unintentional interception; and

    - Clarification, in view of recent court judgments, of the treatment of stored communications, specifically with regard to unauthorised accessing of voicemails.

Equipment Interference

The draft Equipment Interference Code of Practice applies to the activities of the Security and Intelligence Agencies in the UK and overseas. The draft Code explains when the Security and Intelligence Agencies can lawfully interfere with electronic equipment, such as computers, and the rules and safeguards that govern the use of any information obtained by these means. It sets out the procedures that must be followed before such interference can take place, the processing, retention, destruction and disclosure of any information obtained by means of the interference, and the independent oversight provided by the Intelligence Services Commissioner.

As equipment interference is essentially a type of property interference, the draft Code is similar to the existing published guidance in the Covert Surveillance and Property Interference Revised Code of Practice regarding the process for authorising equipment interference, record keeping, oversight and complaints. The draft Code also mirrors the handling safeguards for intercepted material in the Interception Code of Practice and introduces guidance relating to the authorisation of equipment interference outside the UK under section 7 of the Intelligence Services Act 1994.

Responses to this consultation, or a summary of such responses, may be published (with the permission of the respondent) in the interest of ensuring an informed and transparent debate.