Home Office

Regulation of Investigatory Powers Act

Government Response: Interception of Communications and Equipment Interference Codes of Practice Public Consultation

November 2015

Introduction and the legislation

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 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.

On 4 November 2015 the Government published new legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers for pre-legislative scrutiny by a Joint Committee of Parliament, with the intention of introducing a Bill early in 2016. The new legislation must be enacted before the sunset provision in the Data Retention and Investigatory Powers Act 2014 takes effect on 31 December 2016.

Consultation

On 6 February 2015 the Home Office launched a consultation on proposals to:

1) Update the Interception of Communications Code of Practice which regulates the powers and duties conferred or imposed under Chapter 1 of Part 1 of RIPA, which provides for the interception of communications. The updated code reflected developments in the law since the code was brought into force in 2002. It also provided more information on the safeguards that apply to the security and law enforcement agencies' exercise of interception powers.

   The key changes to the code were:

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

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

- It included changes to reflect provisions in the Data Retention and Investigatory Powers Act 2014 (DRIPA). Specifically, the code provides guidance on service of warrants and notices on communication service providers outside the UK and reflects the clarification of the existing definition of "telecommunications service" in RIPA which makes clear that internet based services are included.

2) Publish a new Equipment Interference Code of Practice which 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.

Together, these codes of practice made more information publically available about the stringent safeguards that the Security and Intelligence Agencies apply in their use of Investigatory Powers and how the Security and Intelligence Agencies are held to account by the Independent Commissioners who oversee their activity.

Responses to the Consultation

Following the publication of the draft codes on 6 February 2015, 135 replies were received. 101 replies were based on a common script produced by an interested party.

The following bodies contributed to the consultation:

National Union of Journalists
News Media Association

Faculty of Advocates
Law Society of Scotland
Law Society
Bar Council
Criminal Bar Association
Reprieve
Open Rights Group and Privacy International
Liberty
Access, Center for Democracy & Technology
Linx
Tech UK
All Party Parliamentary Group on Drones (APPG)
Sky UK Ltd
BT
Big Brother Watch
GreenNet

This document summarises the main responses and comments that informed revisions to the codes.

The responses are listed below in three sections:

- The Interception of Communications Code of Practice.
- The Equipment Interference Code of Practice.
- Responses relating to the protection of confidential information, including communications subject to legal professional privilege, which applied to both codes.

Principal comments relating to the Interception of Communications Code of Practice

We received a range of comments relating to the Interception of Communications Code of Practice and have set out below the key themes which form the bulk of the comments and how, where appropriate, they have been addressed in the code.

Interception

Comments:

Several respondents raised concerns about the operation of the framework for the interception of communications in general. Common themes were that RIPA is no longer fit for purpose in a digital age, that the oversight regime should be strengthened (including judicial authorisation for warrants) and that there should be greater transparency around the exercise of interception powers and the safeguards which are in place against their misuse. Comments were also raised about the utility of the regime for external interception under s.8(4) of RIPA, specifically in relation to its necessity and proportionality and the distinction between internal and external communications.

Response:

On 4 November 2015 the Government published legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers for pre-legislative scrutiny by a Joint Committee of Parliament, with the intention of introducing a Bill early in 2016. This builds on three comprehensive reviews covering investigatory powers, privacy and security from David Anderson QC, the independent reviewer of terrorism legislation; the Intelligence and Security Committee and the Royal United Services Institute.

Intelligence-sharing

Comments:

A small number of respondents have called for safeguards to govern the issue of intelligence sharing with the UK's intelligence partners.

Response:

The draft code published in February contained protections for the dissemination of material intercepted by UK Agencies. Further detail has since been added to the code to make clear the safeguards that apply where intercepted material is disclosed to the authorities of a country or territory outside the UK.

To address concerns about bulk intelligence gathering the Government has added a new chapter providing guidance on the safeguards that apply where requests are made to international partners for intercepted material.

Amendments to reflect DRIPA

Comments:

Some respondents expressed concerns about additions to the code which reflected provisions in the Data Retention and Investigatory Powers Act 2014. Firstly, respondents were concerned that requiring CSPs outside UK jurisdiction to comply with an interception warrant may place them in breach of the laws of their host state. Secondly, respondents have suggested that the amended definition of telecommunications services has extended the scope of RIPA and is not sufficiently clear. It has been suggested that the code should list each current technology that the Government considers to be a telecommunication service.

Response:

These concerns cannot be addressed through a code of practice. Parliament will have the opportunity to consider the legislative framework for interception in the context of the Investigatory Powers Bill.

Principal comments relating to the Equipment Interference Code of Practice

We received a range of comments relating to the Equipment Interference Code of Practice and have set out below the key themes which form the bulk of the comments and how, where appropriate, they have been addressed in the code.

Primary legislation not codes of practice

It was suggested that an overhaul of legislation governing oversight of Intelligence and Security Services interference capabilities, including equipment interference, is needed. A common view expressed was that a code of practice was not a suitable vehicle for setting out the power to conduct equipment interference and that it should be provided for in primarily legislation. This would offer an opportunity to have an open and transparent debate about the use of equipment interference by the Security and Intelligence agencies.

Response:

On 4 November 2015 the Government published legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers for pre-legislative scrutiny by a Joint Committee of Parliament, with the intention of introducing a Bill early in 2016. This builds on three comprehensive reviews covering investigatory powers, privacy and security from David Anderson QC, the independent reviewer of terrorism legislation; the Intelligence and Security Committee and the Royal United Services Institute.

Security of computers and networks

Concerns were raised about how equipment interference affects the security of computer networks and devices.

Response:

The Security and Intelligence Agencies take their role in relation to internet security seriously. GCHQ for example, has an important information assurance role, providing advice and guidance to enable Government, industry and the public to protect their IT systems and use the internet safely. To ensure that Secretaries of State understand the potential impact of equipment interference and can be confident that the warrants they authorise are necessary and proportionate, paragraph 4.6 of the code now states that each application for an equipment interference warrant should contain *"any action which may be necessary to install, modify or remove software on the equipment, including an assessment of the consequences (if any) of those actions."*

Overhaul of the warrantry process

Similar to comments raised about interception, some respondents expressed concerns about the warranty oversight regime. In particular, they argued it should be strengthened to include the introduction of judicial authorisation for warrants as an additional check.

Government response:

This is not an issue that can be addressed through a code of practice. As set out above, new legislation on investigatory powers will seek to offer greater clarity, transparency and safeguards. This issue will be considered in the context of the new legislation.

Safeguards for keeping records and handling information

It was suggested that keeping records and the handling of information could be strengthened and clarified. There was particular concern about how we share information obtained via equipment interference with intelligence partners and requests to make this subject to stricter statutory controls.

Government response:

We are confident that the code provides sufficient safeguards in relation to the handling and dissemination of material obtained by equipment interference. The circumstances in which the Security and Intelligence Agencies can disseminate information is defined in chapter 6 of the code. Paragraph 6.5 states that “the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services’ functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act.” Paragraph 6.6 of the code states that the “number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services’ functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service.” To add clarity, however, in addition to the list set out in Chapter 5 of the code, it has been amended to require all applications and renewals for warrants, and the details of what equipment interference has occurred, to be centrally retrievable for at least the next three years.

Comments relating to the interception or acquisition through equipment interference of 'confidential information'

Many of the responses to the consultation were concerned wholly or in part with the interception or acquisition through equipment interference of communications subject to legal privilege.

Communications subject to legal privilege - general

Comments:

Some respondents asserted that lawyer-client confidentiality should be protected in primary legislation by making clear that the deliberate targeting of lawyers' communications is unlawful.

Government response:

The Government fully acknowledges the importance of lawyer-client confidentiality, which is why there are already robust safeguards in place governing the acquisition and handling of communications subject to legal privilege. However, the Government believes that it can be necessary for the intelligence and law enforcement agencies to target communications between lawyer and client in order to counter a serious threat to national security or to protect a person from serious harm. This is why the Regulation of Investigatory Powers Act 2000 (RIPA) and the interception and equipment interference codes do not place an absolute bar on the interception/ acquisition of legally privileged communications. It is vitally important that we do not unduly fetter the important work of the police and the security and intelligence agencies in their efforts to catch serious criminals and to prevent terrorist attacks.

The legal basis for the interception of communications is set out in Chapter 1, Part 1 of RIPA. This stipulates that interception must be authorised by a Secretary of State, can only be undertaken by a limited number of agencies, and for one of three statutory purposes. It can only be used when the Secretary of State is satisfied that it is necessary and proportionate, and that there is no other means available to achieve the same end. Similarly, the corresponding authorisation process and safeguards for equipment interference are set out in the section 5 and 7 of the Intelligence Services Act. Specific safeguards governing the retention and dissemination of legally privileged communications gained via equipment interference or interception are set out in statutory codes of practice.

Comments:

Some respondents argued that the best way to protect the principle of legal privilege is to require the Secretary of State to obtain judicial authorisation before issuing a warrant.

Government response:

This issue is not one that can be addressed through codes of practice. Parliament will have the opportunity to consider the legislative framework for interception in the context of the Investigatory Powers Bill.

Communications subject to legal privilege – text in the codes

Comments:

Several respondents suggested detailed amendments to the codes to introduce further safeguards for the retention and dissemination of legally privileged communications gained via interception and equipment interference. The following measures were proposed:

- Inclusion of a presumption that any communication between lawyer and client is privileged unless the contrary is established.

- A requirement for advice to be sought from a legal adviser where there is doubt as to whether communications are subject to legal privilege.

- A requirement for the Secretary of State to consider whether the purpose of the proposed interception or equipment interference could be served by obtaining non-privileged information.

- Addition of a statement that guidance in the codes relating to the protection of legally privileged communications takes precedence over any contrary content of an Agency's internal guidance.

- Removal of the caveat which allows for material subject to legal privilege to be acted on without consulting a legal adviser in exceptional and compelling circumstances.

- Clarification that not only are there no circumstances in which lawyers and policy officials may rely on legally privileged communications in order to gain a litigation advantage (as was clear in the pre-consultation version of the code) but they should not even have sight of such material.

- Apply consideration of how likely it is that communications subject to legal privilege will be intercepted to the selection of communications under s.8(4). Likewise, the 'exceptional and compelling circumstances' test which applies to the application process for section 8(1) warrants where the intention is to acquire such communications should also apply to the selection of communications under s.8(4).

Government response:

We recognise the importance of this issue and have incorporated these measures into the codes (chapter 4 of the interception code and chapter 3 of the equipment interference code). In most cases the suggestions make explicit or clarify safeguards which previously existed. Together they further strengthen the protections afforded to legally privileged material.

Comments:

A small number of respondents felt that if deliberate targeting of legally privileged material is to be permitted, the threshold must be set at a higher level of "imminent threat of death or serious injury or a serious threat to national security."

Government response:

The Government is satisfied that the threshold in the code, “threat to life or limb or to national security, and the interception / equipment interference is reasonably regarded as likely to yield intelligence necessary to counter the threat” is sufficiently high.

Comments:

A small number of respondents argued for the inclusion of technical safeguards such as bin-lists that automatically exclude legally privileged communications from interception under a s.8(4) warrant.

Government response:

This suggestion misinterprets the nature of s.8(4) interception. The s.8(4) regime envisages that a volume of intercepted material will be generated by the act of interception pursuant to a s.8(4) warrant. The volume may be substantial. A much smaller volume of intercepted material can then be authorised to be selected to be read, looked at or listened to. In order to give effect to this proposal it would be necessary to add the telephone numbers and emails addresses of every legal firm in the UK to a bin-list system. Even if this were technically possible, it would be impractical and damaging to national security.

Comments:

A small number of respondents felt that the codes should include information about the policies of individual intelligence agencies.

Government response:

Chapter 4 of the Interception Code and chapter 3 of the Equipment Interference Code summarises and signposts the policies that the relevant Agencies have in place for the protection of legally privileged communications. It would not be in the interests of national security to disclose each Agency’s internal operational guidance.

Comments:

A small number of respondents suggested that any intercepted legally privileged material should be delivered to claimants engaged in litigation against the Government.

Government response:

Disclosure of the existence of a warrant is prohibited by s.19 RIPA.

Comments:

A small number of respondents said that there was no explanation for why a new interception code was necessary and felt that a code of practice is not an appropriate vehicle for making information publically available.

Government response:

The Interception of Communications Code of Practice regulates the powers and duties conferred by RIPA and sets down procedures to be followed by public authorities. It is right that it contains information about the safeguards which apply so that the public may understand the ambit of the powers and safeguards applied to the exercise of interception powers.

Other confidential communications

Comments:

A small number of respondents raised concerns about the adequacy of protections for journalistic material. It was suggested that there should be further guidance about the consideration which should be given prior to the authorisation of interception of journalistic communications and stronger protections against the disclosure of journalistic communications which have been intercepted. A further concern was raised about the protection for communications between MPs and their constituents.

Government response:

The codes state that particular consideration must be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business.

Chapter 5 of the Interception of Communications Code of Practice makes clear the safeguards that apply to targeted interception in general, including that a warrant may only be issued by a Secretary of State and providing this is necessary and proportionate in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic wellbeing of the UK (if relevant to the interests of national security). It also explains that each targeted warrant application should include consideration of whether the communications might affect journalistic confidentiality. Chapter 4 sets out specific safeguards that apply to this category of communications.

Similar safeguards apply to material gained via equipment interference and are set out in chapter 3 of the Equipment Interference Code of Practice.