Home Office

# NATIONAL SECURITY NOTICES
# DRAFT Code of Practice

Pursuant to Schedule 7 to the Investigatory Powers Act [ ]

[Autumn] 2016

# National Security Notices
## DRAFT Code of Practice



Published for consultation alongside the Investigatory Powers Bill

[Autumn] 2016

Contents

# 1. Introduction

1.1 This Code of Practice relates to the powers and duties conferred or imposed under sections 228, 230, 231, 232 and 233 of Part 9 of the Investigatory Powers Act 2016 ("the Act"). It provides guidance on the procedures to be followed when a national security notice is given. This Code of Practice is intended to set out further detail on the circumstances in which a national security notice can be given; the process that must be followed before a notice can be given; the obligations that are imposed by the service of a notice and the ensuing right of review; and oversight of the use of national security notices.

1.2 The Act provides that all Codes of Practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act, it must be taken into account.

1.3 For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of an intercepting agency's internal advice or guidance.

# 2. Scope and definitions

## What is a national security notice?

2.1 Section 228 of the Act provides that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of such specified steps as are considered necessary in the interests of national security. A notice can be given only if the Secretary of State is satisfied that the steps required are necessary and proportionate. Detail on the definition of a telecommunications operator is provided later in this chapter.

2.2 The power to give a notice under section 228 replaces in part the power that was contained in section 94 of the Telecommunications Act 1984 which has been used for a range of purposes including for civil contingencies and to acquire communications data in bulk. Powers to acquire communications data in bulk are now contained in Chapter 2 of Part 6 of the Investigatory Powers Act. Part 1 of Schedule 9 to the Investigatory Powers Act repeals section 94 of the Telecommunications Act.

2.3 Chapter 3 provides information on the type of support that may be required by a national security notice.

2.4 Section 228 makes clear that a national security notice cannot be used for the primary purpose of interfering with privacy, acquiring communications or data where a warrant or authorisation is available under the Act. In any circumstance where a notice would involve the acquisition of communications or data as its main aim, and an additional warrant or authorisation provided for elsewhere in the Act (or in other legislation such as part two of the Regulation of Investigatory Powers Act 2000 (RIPA), the Intelligence Services Act 1994 (ISA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)) is available, it would always be required. As such, a notice of itself does not authorise an intrusion into an individual's privacy, where that is the primary purpose. More detail on this is provided in Chapter 3.

## What is a telecommunications operator?

2.5 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is in, (in whole or in part), or controlled from the UK. These definitions make clear that obligations in the Part of the Act to which this code applies cannot be imposed on providers whose equipment is not in or controlled from the UK and who do not offer or provide services to persons in the UK.

2.6 Section 237 of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the telecommunication

service provider); and defines 'telecommunications system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the UK or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definition of 'telecommunications service' in the Act is intentionally broad so that it remains relevant for new technologies.

2.7 The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunications system is included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.8 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may only be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if, and in so far as, it provides a messaging service.

.

# 3. National Security Notices – general rules

## The activity authorised by a notice

3.1 Section 228 of the Act states that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of specified steps as are considered necessary in the interests of national security. A notice can only be given if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by the conduct.

3.2 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 as defined in section 1 of the Civil Contingencies Act 2004. An emergency is described in that Act as:

a) An event or situation which threatens serious damage to human welfare in the UK

b) An event or situation which threatens serious damage to the environment in the UK

c) War, or terrorism, which threatens serious damage to the security of the UK

3.3 It is not possible to give a list of the full range of the steps that telecommunications operators may be required to take in the interests of national security; not only would this affect the ability of the police and security and intelligence agencies to carry out their work, but as communications technology changes the Secretary of State will need to retain flexibility to respond. However, a notice may typically require a telecommunications operator to provide services to support secure communications by the 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.

## Necessity and proportionality

3.4 The giving of a national security notice can only be justified if the steps it requires are necessary for a legitimate purpose and proportionate to that purpose. The Act recognises this by requiring that the Secretary of State believes that the steps required by the notice are necessary in the interests of national security.

3.5 The Secretary of State must also believe that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the reasonableness of the steps that must be taken

against the need for the activity in protecting national security. Each action authorised should bring an expected benefit and should not be disproportionate or arbitrary.

3.6 A national security notice cannot be used for the primary purpose of interfering with privacy, acquiring communications or data. In any circumstance where a notice would involve the acquisition of communications or data as its main aim, an additional warrant or authorisation provided for elsewhere in the Act (or in RIPA, ISA or RIP(S)A) would always be required. Such authorisation would require an assessment of the necessity and proportionality of the intrusion into privacy. However, there may be very limited circumstances where data might incidentally be acquired through the activity authorised by a national security notice where there isn't a suitable additional warrant or authorisation that could be sought to authorise its acquisition. In those circumstances, the Secretary of State must, in authorising the conduct required in the notice, consider whether it is necessary and proportionate for this data to be acquired incidentally.

3.7 This code does not contain particular provision designed to protect the public interest in the confidentiality of journalistic information and any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information, because a notice does not authorise acquiring this information.

## Format of national security notice applications

3.8 Responsibility for the issuing of national security notices rests with the Secretary of State. An application to be made to the Secretary of State for a national security notice to be given to a telecommunications operator should contain the following information:

a) The purpose of the notice and what it seeks to achieve;

b) Why it is not possible to achieve the required outcome by using one of the other powers contained in the Investigatory Powers Act;

c) How the activity required by the notice is proportionate to what it seeks to achieve;

d) Whether the activity proposed is likely to interfere with an individual's privacy;

e) An assessment of the reasonableness of the steps the telecommunications operator is required to take, and details of the consultation that has taken place with the telecommunications operator to whom the notice will be given.

3.9 Where the application for a notice identifies that an interference with privacy may occur because personal data may be acquired, the application must make clear that an authorisation to approve the interference with privacy has been obtained. If the interference with privacy is incidental to the national security notice, the application must make that clear and seek the Secretary of State's approval for the interference. The application must therefore:

i. Set out known/expected interference or where there is a potential for interference to occur;

ii. Explain why the interference is necessary and;

iii. Describe any mitigating action which will be taken to keep the interference to a minimum.

3.10 An example of what should be contained in an application for a national security notice is attached at Annex A.

## Authorisation of a national security notice

3.11 The Secretary of State may only give a notice under section 228 if the Secretary of State considers the following tests are met:

- **The notice is necessary in the interests of national security;**
- **The conduct authorised by the notice is proportionate to what it seeks to achieve;**
- **Any interference with privacy is authorised** by an appropriate authorisation under the Investigatory Powers Act (or other statute where appropriate) or, where it is incidental and cannot be authorised by other means, it is necessary and proportionate to what the notice seeks to achieve; and
- **There are satisfactory safeguards in place.**

- **Judicial Commissioner approval.** The Secretary of State may not give a notice unless and until the decision to give the notice has been approved by a Judicial Commissioner. Section 230 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the notice is necessary, and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

## Duration and Review of National Security Notices

3.12 A national security notice remains in force until it is cancelled. The Secretary of State must keep a notice under review. At six monthly intervals, the Secretary of State must consider whether the activity required by the notice remains necessary and proportionate. As part of the review, the Secretary of State must consider whether any incidental interference with privacy remains necessary and proportionate and should continue to be authorised by the notice and not an alternative authorisation provided for in the Investigatory Powers Act or in other relevant statutes. The review must also consider whether any incidental interference with privacy has occurred since the last review that was not anticipated, and the Secretary of State must be satisfied that any continued interference is justified, and should not be authorised by alternate means.

3.13 The Secretary of State must cancel the notice if the conduct it requires is no longer necessary or proportionate.

# 4. The giving of a notice and telecommunications operator compliance

4.1 After a notice has been authorised, it is given to the telecommunications operator. Where it is given to anyone providing a telecommunications service, or who has control of a telecommunication system in the UK, that person is under a duty to take all the steps required by the notice. This applies to any company in the UK. Section 231 sets out the means by which that duty may be enforced.

4.2 An example of what a national security notice will look like is contained at Annex B. It is necessarily blank so as not to reveal sensitive capabilities and undermine their effectiveness.

## Consultation with operators

4.3 Before giving a notice, the Secretary of State must consult the operator[1]. In practice, consultation is likely to take place long before a notice is given. The Government will engage with an operator who is likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

4.4 In the event that the Secretary of State considers it appropriate to give a notice, the Government will take steps to consult the telecommunications operator formally before the notice is given. Should the person to whom the notice is to be given have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

## Matters to be considered by the Secretary of State

4.5 Following the conclusion of consultation with a telecommunications operator, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is justified and that proper processes have been followed.

4.6 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 231(3):

- The likely benefits of the notice – this may take into account projected as well as existing benefits.

[1] See section 231(2).

- The likely number of users of any telecommunications service to which the notice relates, if known.

- The technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator.

- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.

- Any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

4.7 In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision.

4.8 The notice must specify the period within which the steps specified in the notice are to be taken. The Secretary of State must consider that period to be reasonable.

## Receiving a notice

4.9 Once the Secretary of State has made a decision to give a notice, and the decision has been approved by the Judicial Commissioner, arrangements will be made for it to be given to the telecommunications operator. During consultation, it will be agreed who within the company should receive the notice and how it should be provided (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be given to a senior executive within the company.

4.10 A person to whom a national security notice is given is under a duty to comply with the notice. The duty to comply with a national security notice is enforceable against a person in the UK by civil proceedings brought by the Secretary of State[2].

## Disclosure

4.11 Any person to whom a national security notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[3].

[2] See section 231(10)(a).

[3] See section 231(8)

## Contribution to the costs of taking the steps required by a national security notice

4.12 Section 225 of the Act recognises that operators incur expenses in complying with requirements in the Act, including steps taken in response to a national security notice. The Act, therefore, allows for appropriate payments to be made in respect of these costs.

4.13 Public funding and support is made available to operators to ensure that they can provide, outside of their normal business practices, the support that is required by a national security notice.

4.14 It is legitimate for an operator to seek contributions towards its costs which may include an element providing funding of those general business overheads required in order to take the steps specified by a national security notice.

4.15 This is especially relevant for operators which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems.

4.16 Contributions may also be appropriate towards costs incurred by an operator which needs to update its systems to maintain, or make more efficient, the support required by a national security notice. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements specified in the notice.

4.17 Any operator seeking to recover appropriate contributions towards its costs should make available to the Government such information as the Government requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the operator.

4.18 Any operator that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

## Referral of national security notices

4.19 The Act includes clear provisions for the recipient of a notice to request a review of the requirements placed on them in a national security notice should they consider these to be unreasonable. A person may refer the notice back to the Secretary of State for review under section 233 of the Act.

4.20 The circumstances and timeframe within which a telecommunications operator may request a review are set out in regulations made by the Secretary of State and approved by Parliament. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is given.

4.21 Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Judicial Commissioner will consider whether the notice is proportionate.

4.22 Both bodies must give the relevant telecommunications operator and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions.

4.23 After considering reports from the TAB and the Judicial Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State's decision is to confirm the effect of the notice, this decision must be approved by the Investigatory Powers Commissioner (IPC). Until this decision is made and approved by the IPC, there is no requirement for the telecommunications operator to comply with those part of the notice that have been referred.

## Revocation of national security notices

4.24 A national security notice must be revoked (in whole or in part) if it is no longer necessary to require a telecommunications operator to provide a national security capability as at section 232.

4.25 Circumstances where it may be appropriate to revoke a notice include where an operator no longer operates or provides the services to which the notice relates, where operational requirements have changed, or where such requirements would no longer be necessary or proportionate.

4.26 The revocation of a national security notice does not prevent the Secretary of State giving a new notice, covering the same, or different services, to the same operator in the future should it be considered necessary and proportionate to do so[4].

[4] See Section 232(8)

# 5. Oversight

5.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ('the Commissioner'), whose remit is to provide comprehensive oversight of the use of the powers contained within Part 9 of the Act and adherence to the practices and processes described by this code. By statute the Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work.

5.2 The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. Section 207(3) sets out that the IPC must keep under review the giving and operation of national security notices. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on his or her own initiative or they may be asked to investigate a specific issue by the Prime Minister.

5.3 The IPC will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers must, by law, offer all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

5.4 The Commissioner must report annually on the findings of their inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the national interest. Only the Prime Minister will be able to authorise redactions to the Commissioner's report. If the Commissioner disagrees with the proposed redactions to his or her report then the Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

5.5 The Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and telecommunications operators may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce guidance for public

authorities on how to apply and use Investigatory Powers. Wherever possible this guidance will be published in the interests of public transparency.

5.6 Anyone working for a public authority or communications service provider who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner, who will consider them. In particular, any person who exercises the powers described in the Act or this code must report to the Commissioner any action undertaken which they believe to be contrary to the provisions of this code. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority. The Commissioner may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the Investigatory Powers Tribunal (IPT).

5.7 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

# Annex A: Detail which must be contained in a national security notice application

**National security notice application**

An application to the Secretary of State for a national security notice should set out:

- The likely benefits of the notice – this may take into account projected as well as existing benefits.
- The likely number of users of any telecommunications service to which the notice relates, if known.
- The technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator.
- The likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money.
- Any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

An application should also address the following questions:

Necessity

- **What is the purpose of the notice/ what are you seeking to achieve?** *[Brief description of what the telecommunications operator will be asked to do and why it is necessary in the interest of national security]*
- **Can the same result be achieved using any other statute or other powers in the Investigatory Powers Act?** *[if so, explain why a national security notice is the most appropriate means of achieving the objective]*

Proportionality

- **How is the conduct required by the notice proportionate to what you are seeking to achieve?** *[the application must set out how what the telecommunications operator is being asked to do is proportionate to the objective sought]*

- **Will the activity proposed interfere with an individual's privacy?** *[The application must set out: known/expected interference or where there is a potential for interference to occur; explain why the interference is necessary and; describe any mitigating action which will be taken to keep the interference to a minimum. Where the main purpose is interference with privacy an appropriate authorisation under the Investigatory Powers Act must be sought if one is available. If the interference is incidental or there is no alternative means of authorising, the application must make that clear and seek the Secretary of State's approval for the interference]*

- **Is it reasonable to require the operator to take the steps set out in the notice? Have you consulted the telecommunications operator on whom the notice will be given?** *[The application should highlight any concerns which have been expressed by the intended recipient and describe what action has been/can be taken to mitigate their concerns. The application should also set out the period within which the steps specified in the notice are to be taken and an assessment of why that period is reasonable. ]*

- **Is the telecommunications operator on whom the notice is to be given uniquely placed to undertake the activity required by the notice or are other operators subject to similar obligations?**

# Annex B: Example of a national security notice

**NATIONAL SECURITY NOTICE**
**UNDER SECTION 228(1) OF THE INVESTIGATORY POWERS ACT [ ]**

*[Insert telecommunications operator's name]*

1. In exercise of the power conferred by section 228 of the Investigatory Powers [Act 2016] the Secretary of State considers that it is necessary to require *[insert telecommunications operator's name]* to take the steps set out in this notice. A Judicial Commissioner has approved the Secretary of State's decision.

2. The requirements set out in paragraph 5 of this notice are necessary in the interests of national security and proportionate to what is being sought to be achieved.

3. *[insert telecommunications operator's name]* must :

   a. **[Having appropriate systems in place to carry out the task required]**

   b. **[Issuing instructions to staff which achieve the requirements set out in article 3]**

4. The requirements and results referred to in paragraph 2 are:

   a. **[List the specific tasks which the operator is required to undertake in support of the notice]**

   b.

   c.

5. The steps set out in paragraph 5 must be taken by [date].

6. [insert other information as necessary relating to the operation of the direction].

7. Insert one of the following statements:
   a. no private/personal data will be acquired as a result of the activity required by this notice

b. any private/personal data acquired as a result of the activity required by this notice has been authorised under *[insert as required] or*
c. any private/personal data acquired as a result of the activity required by this notice is incidental and hereby authorised

8. The direction(s) given to *[insert telecommunications operator's name]* by the Secretary of State under section 94 of the Telecommunications Act 1984

Or

The notice given to [*insert telecommunications operator's name]* under section 228 of the Investigatory Powers Act [ ]

is revoked.

In accordance with section 233 of the Investigatory Powers Act [ ], *[insert telecommunications operator's name]* may seek a review of this notice

Signed……..
Her Majesty's Secretary of State for [the Home Department]
Dated