Home Office

Investigation of Protected Electronic Information

Code of Practice

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

Investigation of Protected Electronic Information

Code of Practice

Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000

LONDON: TSO

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone 0870 240 3701

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

TSO@Blackwell and other Accredited Agents

Published for the Home Office under licence from the Controller of Her Majesty's Stationery Office.

ISBN 978-1-84-726202-8

First Impression 2007

Printed in the United Kingdom for TSO

N5665831 C40 10/07

Contents

Chapter 1
INTRODUCTION

1.1 This code of practice relates to the powers and duties conferred or imposed under Part III of the Regulation of Investigatory Powers Act 2000 ('the Act'). It provides guidance to be followed when exercising powers under Part III of the Act ('Part III') to require disclosure of protected electronic information (electronic data) in an intelligible form or to acquire the means by which protected electronic information may be accessed or put in an intelligible form.

1.2 This code applies to the exercise and performance by any person (other than a judicial authority or a person holding judicial office) of the powers and duties conferred or imposed by or under Part III.

1.3 The code should be readily available, in written or electronic form, to members of any public authority involved in the investigation of protected electronic information and to persons upon whom any duty is imposed under Part III of the Act.

1.4 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under the Act ('the Investigatory Powers Tribunal'), or to one of the Commissioners responsible for overseeing the powers conferred by the Act, it must be taken into account.

1.5 The exercise of powers and duties under Part III is kept under review by the Commissioners appointed under sections 57, 59 and 62 of the Act ('the Commissioners').

1.6 This code extends to the United Kingdom.

Chapter 2
BACKGROUND

2.1 Information security technologies have allowed electronic commerce to flourish, enabling businesses and individuals to secure and protect their electronic data and to maintain the privacy of their electronic communications. Individuals going about their lawful business, both openly and privately, use these technologies every day.

2.2 Terrorists and criminals use the same technologies to protect their electronic data and the privacy of their electronic communications, to conceal evidence of their unlawful conduct and to evade detection or prosecution.

2.3 At its simplest the protection of electronic data is undertaken using a password which, if correct, gives access to the data in an intelligible form. More complex applications use cryptography both to protect access to the data and to put the data itself into a form that is unintelligible without the correct password or key.

2.4 Cryptographic technologies, which have been essential to the success of e-commerce and online businesses, have various uses:

- **Authentication** – guaranteeing that the originator or recipient of data is the person they claim to be;
- **Availability** – assurance that the systems responsible for delivering, storing and processing data are accessible when needed, by those who need them
- **Confidentiality** – protecting data to ensure that its contents cannot be read by anyone other than an intended recipient;
- **Integrity** – guaranteeing that data has not been accidentally or deliberately corrupted;
- **Non-repudiation** – preventing the denial of previous commitments or actions

2.5 Primarily it is application of cryptography to the confidentiality of data which is exploited by terrorists and criminals to protect their data, whether it is stored data, on a disk or other storage device, or data being communicated from one to another or from one to many others. The measures in Part III are intended to ensure that the ability of public authorities to protect the public and the effectiveness of their other statutory powers are not undermined by the use of technologies to protect electronic information.

Chapter 3
SCOPE OF THE POWERS

3.1 Part III provides a statutory framework that enables public authorities to require protected electronic information which they have obtained lawfully or are likely to obtain lawfully be put into an intelligible form; to acquire the means to gain access to protected information and to acquire the means to put protected information into an intelligible form.

3.2 The specific provisions are:

- power to require disclosure of protected information in an intelligible form (section 49);
- power to require disclosure of the means to access protected information (section 50(3)(c);
- power to require disclosure of the means of putting protected information into an intelligible form (section 50(3)(c)), and
- power to attach a secrecy provision to any disclosure requirement (section 54).

3.3 Failure to comply with a disclosure requirement or a secrecy requirement is a criminal offence.

3.4 Public authorities that use, or seek to use, the provisions in Part III will do so with the objective of securing necessary access to lawfully acquired protected information in an intelligible form, and, where necessary and proportionate to do so, to seek or to require assistance to do that.

3.5 In practice this means that investigators must take into account the legitimate needs of businesses and individuals to maintain the integrity of their information security management processes and will, wherever practical, require the disclosure, or seek assistance to secure the disclosure, of protected information in an intelligible form.

3.6 When exceptional circumstances do arise, access to protected information in an intelligible form may be achieved more readily by securing the application of an established process to the data rather than requiring the disclosure of key material and creating a bespoke decryption facility where the processing may, even then, be undertaken by a technically competent employee of a firm or business under supervision of the investigator. Processing data the way it would have been processed ordinarily, in so far as that is practical, will also reduce costs and minimise any potential collateral intrusion.

3.7 Requiring the disclosure of the means to access protected information or to put it into an intelligible form should be undertaken only where the investigator, or the person able to grant permission to impose that requirement, reasonably believes that assistance to make the protected information available in an intelligible form or in compliance with a requirement to disclose the protected information in an intelligible form is unlikely to be forthcoming or effective.

3.8 Consequently use of the power to require disclosure of key material can be expected to be used only where a person who is able to put the protected information into an intelligible form indicates or suggests that he will not exercise that ability either voluntarily or upon compulsion. In practice this means the power is more likely to be exercised in relation to individuals who are the subject of investigation and are responsible for protecting information which is believed to be evidence of unlawful conduct or relevant material to the investigation.

3.9 The National Technical Assistance Centre (NTAC),[1] which provides technical support to public authorities, particularly law enforcement agencies and the intelligence services, includes a facility for the complex processing of lawfully obtained protected electronic information.

3.10 NTAC is the lead national authority for all matters relating to the processing of protected information into intelligible form and to disclosure of key material. All public authorities should consult with NTAC at the earliest opportunity when considering the exercise of

1 NTAC may be contacted at: ripaiii@ntac.gsi.gov.uk

the powers in Part III. No public authority may serve any notice under section 49 of the Act or, when the authority considers it necessary, seek to obtain appropriate permission without the prior written approval of NTAC to do so. Such approval may be given in specific cases or it can be given to a public authority if NTAC assesses the authority is competent to exercise the powers in Part III.

3.11 In this way NTAC will support public authorities to ensure that the exercise of the powers in Part III is undertaken appropriately, expertly and with the highest regard for compliance with the requirements and principles of the Act and this code. The role of NTAC as a guardian and gatekeeper of the use of Part III will provide assurance to the Commissioners that the scope for inappropriate use of the powers is mitigated. Equally the Commissioners' oversight extends to NTAC itself.

Protected Information

3.12 Protected information means any electronic data, which, without a key to the data cannot, or cannot readily:

- be accessed, or
- be put into an intelligible form.

3.13 Section 49(1) of the Act describes various means by which protected information has come into, or may come into, the possession of any person within a public authority. This includes information that has been, or is likely to be:

Within the scope of section 49(1)(a) of the Act:

- acquired by exercising a statutory power to seize, detain, inspect, search for property or to interfere with documents or other property;
  - for example, seized under a judicial search warrant under section 8 of the Police and Criminal Evidence Act 1984;
  - for example, disclosed in compliance with a judicial production order under Schedule 1 of the Police and Criminal Evidence Act 1984;

Within the scope of section 49(1)(b) of the Act:

- acquired by the exercise of a statutory power to intercept communications, for example under a warrant issued personally or expressly authorised by the Secretary of State under Chapter I of Part I of the Act;

Within the scope of section 49(1)(c) of the Act:

- acquired by undertaking conduct authorised under section 22(3) of the Act (authorised conduct to obtain communications data);
- disclosed as a result of the giving of a notice under section 22(4) of the Act (notice requiring disclosure of communications data);
- acquired by undertaking conduct authorised under Part II of the Act (whether an authorisation for carrying out directed surveillance under section 28, for carrying out intrusive surveillance under section 32, or for the conduct or the use of a covert human intelligence source under section 29);

Within the scope of section 49(1)(d) of the Act:

- provided to, or disclosed to, a public authority in the exercise of any statutory duty whether or not the provision or disclosure of information was requested;

Within the scope of section 49(1)(e) of the Act:

- acquired lawfully by any of the intelligence services,[2] the police, Serious Organised Crime Agency (SOCA) or HM Revenue and Customs (HMRC) without using statutory powers, including information voluntarily disclosed to those authorities by a member of the public.

3.14 Section 49(1) provides by the words "has come in to the possession of any person .... or is likely to do so" that a public authority can seek permission to give a section 49 notice ('a notice') at the same time as seeking to exercise a statutory power to obtain the information or in anticipation of such action. This will occur in circumstances where

2 The Security Service, the Secret Intelligence Service and GCHQ.

there is an expectation that the information being sought is protected. For example an application for, and the issue of, a search warrant, production order or interception warrant may include reference to protected information likely to be seized, produced or intercepted.

3.15 A notice may be given where a person has appropriate permission[3] and reasonably believes that:

- a key[4] to the protected material is in possession of any person;[5]
- a disclosure requirement in respect of the protected information is necessary:
  - in the interests of national security;[6]
  - for the purpose of preventing or detecting crime;[7]
  - in the interests of the economic well being of the United Kingdom,[8] or
  - for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty;
- the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
- that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice.

---

3 See Section 9 of this code.

4 Examples of the sorts of material that can constitute 'a key' are described in paragraph 3.18 to 3.21.

5 Section 81(1) of Act defines 'person' to include any organisation and any association or combination of persons.

6 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. Where a disclosure requirement is considered necessary in the interests of national security a person in another public authority should not give a notice under the Act where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where that person is a member of a Special Branch or the Metropolitan Police Counter Terrorism Command, or where the Security Service has agreed a notice may be given by a member of another public authority in relation to an operation or investigation which would fall within the responsibilities of the Security Service.

7 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 81(5) of the Act.

8 Where, on the facts of the specific case, there is a connection with national security.

Protected information in an intelligible form

3.16 In the Act and throughout this code references to protected information being 'intelligible' or 'put into an intelligible form' mean restoring the protected information to a condition it was in before being protected, whether by encryption or other process. This will be the condition in which the information or data was originally generated or processed before being protected or any condition it was in before being protected. In other words putting information into an intelligible form can include restoring it to a previously protected form to which further decryption or similar process needs to be applied to the information or data in order to comprehend it fully.

3.17 Information put into its original condition must remain in that condition for a period of time that is sufficient to meet the reasonable needs of the person to whom the disclosure is made. Information is not put into an intelligible form if it is put into its original condition, or restored to a previously protected form, only momentarily or for an unreasonably short period of time.

Description of a key

3.18 A key to data means any key, code, password, algorithm or other data (including any proprietary software or cryptographic process) the use of which, by itself or with another key or keys:

- allows protected electronic data to be accessed, or
- facilitates putting protected electronic data into an intelligible form.

3.19 All manner of material can constitute a key. A key can be a plain language password or pass-phrase. It can include, for example, words, phrases or numbers written on any form of paper, plastic cards bearing numbers, electronic chips or magnetic strips and all forms of removable or fixed media for storing electronic data. It can include intangible material, for example, sounds or movements or comprise biometric data derived from, for example, fingerprint readers or iris scanners. Equally key material can be retained in the memory of an individual.

3.20 Ordinarily, for the purposes of this code and in the exercise of the powers contained in Part III, a key will be specific to protected information described in a corresponding notice.

3.21 Supporting information which takes the form of proprietary software that will render intelligible otherwise unintelligible data or more complex material such as algorithms for either or both encryption and decryption of data, comprising computer code (in written, source or executable form) or a functional description of the algorithm or code is unlikely to be a key that is unique to any specific protected electronic data but may, nonetheless, be a relevant key to such data. As such, any reference to a key or to key material can include supporting information.

3.22 Where supporting information is in the possession of a person, a notice for the disclosure of a key may require the disclosure of such supporting information.

3.23 A person from whom protected electronic data has been lawfully seized or otherwise acquired may not be in possession of supporting information that is the intellectual property or proprietary right of another person.

3.24 Reference to any key includes split-keys which, when used in combination, form a single key. Circumstances can arise where it is necessary to combine several split-keys before protected information can be made accessible or put into an intelligible form. This may require separate notices to be given to those persons holding the split-keys (either all of them or sufficient number of them) to require them, acting together, to provide access to the protected information or disclose it in an intelligible form. Equally a notice may be served on a holder of a split-key who undertakes to seek the assistance of such other persons holding other parts of the key or holding any other part of the key in order to fulfil a requirement to provide access to the protected information or disclose it in an intelligible form.

Electronic signature keys

3.25 Any key intended to be used for the purpose only of generating electronic signatures and which has not in fact been used for any other purpose can never be the subject of a disclosure requirement.[9]

3.26 An electronic signature means anything in electronic form which is incorporated into or logically associated with any electronic communication or other electronic data, generated by the signatory or other source of the data, and which establishes the authenticity of the data, its integrity, or both by providing a link between the signatory or other source and the communication or data.

3.27 Where there are reasonable grounds to believe that a key used as an electronic signature has also been used for confidentiality purposes, that key may be required to be disclosed under the terms of the Act. Particular care must be taken when requiring the disclosure of a key that has been used as a signature key to ensure the key is used only for the purposes described in the disclosure notice.

Multi-use keys

3.28 Multi-use keys are keys used to protect more than one item of information, or have been used for signature purposes as well as for putting information into an intelligible form or for protecting all the communications sent to a person only some of which may be the subject of a disclosure notice. Particular care should be taken when a multi-use key is required to access protected information or to disclose it in an intelligible form. The notice must explain explicitly what is required and that it is proportionate to what is sought to be achieved.[10]

9 See Section 49(9) of the Act.

10 See also paragraph 8.4

Session keys

3.29 Session keys are temporary keys used to encrypt or decrypt communications in a single "session". They are often ephemeral and usually unknown to their users. Even when they are not ephemeral a user may nonetheless have limited ability to generate, regenerate or recall them.

Possession of a key

3.30 Possession of a key by a person ('the person') can include circumstances where the key is in their own possession or in the possession of:

- an employee or other individual under their control, or
- a trusted third party or other service provider and the person has an immediate right of access to it or to have it transmitted or otherwise supplied to him.

3.31 Where the key is, or is contained in, anything which the person, an employee or other individual under their control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search, that key is in the possession of the person. This means the key is, or is in, something to which the person or anyone under their control has lawful access.

3.32 Where more than one person is in possession of the key to protected information, and at least one of those is in possession of that key in his capacity as an officer or employee of a corporate body or firm and another is also an officer or employee of the body, or a partner of the firm (or is the corporate body or firm itself), a notice imposing a disclosure requirement shall not be given to any officer or employee of the body or employee of the firm who is in possession of the key unless that person is a senior officer of the body or a partner of the firm. In this context senior officer means a director, manager, secretary or other similar officer of the corporate body (and where the body is managed by its members a director means one of its members).

3.33 In practice this means notices should be served upon a person holding a position such as company secretary, legal director, chief information officer, information disclosure manager, law enforcement liaison manager, single point of contact or other post designated for the purpose of receiving notices served upon the company or firm.

3.34 Where it appears to a person giving a notice that there is no senior officer of the company, or partner of the firm, or a more senior employee to whom it would be reasonably practicable to give the notice, the notice shall be given to an officer or employee in possession of the key. This means an investigator giving a notice must always seek to give that notice to the most senior officer or employee in possession of the key whether or not any less senior officer or employee of the body, or employee of the firm, would be capable of complying with the disclosure notice.

3.35 The requirements for giving a notice to corporate bodies or firms do not apply where the special circumstances of the case mean that the purpose or purposes for which the notice is to be given would be defeated, in whole or in part, if the notice were required to be given to a senior officer of the company or a partner of the firm or a senior employee to whom it would otherwise be reasonably practicable to give the notice. This can include circumstances where a senior officer of the company or a partner of the firm is the subject of, or connected to, the investigation or operation.

Necessity and proportionality

3.36 Exercise of the powers to require disclosure of protected information; disclosure of the means to access such information or to put it into an intelligible form may amount to interference with an individual's right to respect for their private and family life.

3.37 Such interference will be justifiable under Article 8 of the European Convention on Human Rights and in accordance with the Human Rights Act 1998 only if the conduct being required or taking place is both necessary and proportionate and in accordance with the law. The provisions in Part III are designed to meet the requirements

that such activities are in accordance with law and to provide guidance to ensure that the activities are, in fact, both necessary and take place in a proportionate manner.

3.38 The person giving appropriate permission and, where different, the person with that permission must believe that the imposition of a disclosure requirement by a notice is necessary. They should consider whether other means to obtain the protected information in an intelligible form have failed, or would be bound to fail, for example that the person in possession of the key has not provided voluntarily the protected information in an intelligible form or would not do so.

3.39 He must also believe the imposition of that requirement to be proportionate to what is sought to be achieved by obtaining the disclosure of the protected information in an intelligible form or the disclosure of the means to gain access to the protected information or to put it in an intelligible form – that the disclosure requirement is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right to respect for their private life against the benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

3.40 Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation, or to confidential business-client relationships where a disclosure requirement may be imposed upon a corporate body or firm. An application for appropriate permission to give a notice should draw attention to any circumstances which give rise to a meaningful degree of collateral intrusion.

3.41 Taking all these considerations into account in a particular case, an interference with the right to respect of individual privacy may still not be justified because the adverse impact on the privacy of an individual or group of individuals is too severe.

3.42 Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate.

Chapter 4
RULES ON GIVING OF NOTICES

4.1 There are a number of statutory requirements that must be met before any disclosure requirement is imposed. Primarily only a person with appropriate permission may impose a disclosure requirement upon a person in respect of specific protected information. Schedule 2 to the Act defines persons able to grant appropriate permission, persons capable of having appropriate permission and describes the circumstances in which appropriate permission can be obtained.

Who may give notices?

4.2 Any public authority may, in the exercise of its functions, seek permission to serve a notice in relation to protected information that has already been obtained lawfully or in relation to protected information which is not yet in their lawful possession where they have a reasonable expectation of obtaining it.

Who may notices be served upon?

4.3 Section 49 notices may potentially be served on a wide variety of individuals, bodies or organisations. Individuals using products or services to protect data under their control, and businesses involved in producing or supplying such products or services, or using such technologies themselves could, conceivably, be in a position to disclose protected information in an intelligible form or to disclose a key required to put such information into an intelligible form.

4.4 Disclosure requirements are most likely to be imposed on individuals who have protected information directly relevant to an investigation or operation and are themselves a subject of, or are connected to, the investigation or operation. As a consequence of the way that information protection or cryptographic and other

information technologies work, disclosure requirements may also be imposed on a person who has a relevant key to protected information by virtue of a personal or business relationship with an individual subject of, or connected to, an investigation or operation.

4.5 It is important in all circumstances where a notice is being contemplated that careful consideration is given by the person intending to seek appropriate permission or the person able to give that permission to whether a notice should be given, and if so, who should be given the notice. Where the imposition of a disclosure requirement upon a corporate body or firm is being considered, the person intending to seek appropriate permission must determine that body or firm would be able to comply with the proposed disclosure requirement and must determine which individual it should be served upon. That person may have a role for receiving legal notices and may have, or can call upon, the necessary technical expertise.

4.6 The imposition of a disclosure requirement upon a corporate body or firm without any prior consultation should be undertaken rarely and only in special circumstances. This is principally to be when there are reasonable grounds for believing that to do otherwise would prejudice an investigation or operation including where the corporate body or firm was suspected of complicity in unlawful conduct.

4.7 Prior consultation with a corporate body or firm must address the technical and practical implications for the business of a proposed disclosure requirement. This might include any unduly significant disruption to its business that would, or might, occur and any significant impact on the security of its operations that might expose it and its clients to risk or damages particularly when a requirement for disclosure of key material is being proposed. The business may require reasonable time to consider if it is technically able to meet the proposed requirement and, if so, to agree in what time the requirement can be met and, to the extent relevant, at what cost to the business.

4.8 Ordinarily a notice to a corporate body or firm should be served upon a central point of contact for legal or technical matters and should never be served upon an individual in a local office or branch without reference to that central point of contact.

Application for appropriate permission

4.9 Applications for appropriate permission must be made in writing or electronically to a person able to give appropriate permission, for example a judicial authority or a person holding judicial office. The person making the application will be a person involved in conducting an investigation or operation for a public authority. The applicant may be an individual who is seeking appropriate permission or is seeking the grant of appropriate permission on behalf of another person.

4.10 Persons able to give appropriate permission should not grant permission in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons.

4.11 Persons who grant, or who have, appropriate permission must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the investigation of protected electronic data under Part III of the Act and this code.

4.12 Applications may be made orally in exceptional urgent circumstances[11] but a record of that application must be made in writing or electronically within one working day.

4.13 Applications – the original or a copy of which must be retained by the person with the appropriate permission – must:

- include the name (or designation)[12] and the office, rank or position held by the person making the application;
- where it is different from the applicant, include the name (or designation) and the office, rank or position held by the person for whom appropriate permission is being sought;
- include the operation name (if applicable) to which the application relates;

11 See paragraph 4.34

12 The use of a designation rather than a name will be appropriate only for persons in one of the Intelligence services.

- specify the grounds on which the imposition of a disclosure requirement is necessary whether:
  - in the interests of national security;
  - for the purpose of preventing or detecting crime;
  - in the interests of the economic well-being of the United Kingdom; or
  - for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty (and must identify that power or duty);
- describe the protected information which has been, or is likely to be, lawfully obtained;
- confirm the statutory power or other lawful means by which the protected information has been, or is likely to be, lawfully obtained;
- explain why it is reasonably believed that the person on whom it is intended to serve a section 49 notice has possession of a key or keys to the protected information described in the application;
- explain the scope of the disclosure requirement, why the imposition of that requirement is considered necessary and proportionate to what is sought to be achieved by its imposition;
- provide an assessment of the capability, technical or otherwise, of the person on whom it is intended to serve a notice to undertake the disclosure requirement;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- explain why it is not reasonably practicable to acquire or obtain access to the protected information in an intelligible form by some other method without serving a section 49 notice;
- explain to whom the disclosure will be made, how the disclosed material will be handled, stored and safeguarded from unnecessary further disclosure, and
- identify and explain any urgency for which the proposed disclosure requirement is necessary.

Obtaining appropriate permission

4.14 The decision to grant appropriate permission by a person able to do so shall be based upon information presented to them in an application. The grant of appropriate permission to any person must be in writing or, if not, in a manner that produces a record of it being granted.

4.15 The record of the grant of appropriate permission may take the form of a countersignature to the application, may be separate from that or be included in any warrant or order being given at the same time.

4.16 The exercise of appropriate permission by a person who has that permission by virtue of their rank or holding a designated office or position (in the police, SOCA, HMRC and members of HM forces) may be undertaken by them upon application from a person who would otherwise need to obtain appropriate permission. A record of the decision to exercise appropriate permission by a person who has that permission should be kept in the same way as if permission were being obtained from a person able to grant it.

Format of notices

4.17 The statutory requirements of the Act[13] mean that any notice imposing a disclosure requirement in respect of any protected information:

(a) must be given in writing or in a manner that produces a record which includes the date and time it was given;

(b) must describe the protected information to which the notice relates and, where known and where appropriate, identify any key to the protected information;

(c) must specify the grounds on which the notice is necessary including where appropriate the statutory power or duty within the meaning of section 49 (2) (b) (ii) of the Act;

13 See section 49(4)

(d) must specify the office, rank or position of the individual giving the notice, and where appropriate and helpful to do so, their name (or designation);

(e) must specify the office, rank or position of the person who granted permission for the notice to be given and where appropriate, which will be ordinarily be the name (or designation) of that person. If the person giving the notice does so without another persons' permission, the notice must set out why the person giving the notice is entitled to do so;

(f) must specify the time by which the notice is to be complied with, which must be reasonable in all the circumstances; and

(g) must set out clearly the extent of the disclosure required – whether a disclosure of the protected information in an intelligible form, or a disclosure of the means to either or both access the protected information and put it in an intelligible form – and must set out clearly how the disclosure is to be made.

4.18 A notice cannot require any person to make a disclosure to someone other than the person giving the notice, or such other person as is specified or identified in the notice where disclosure to another person is in accordance with the notice. For example, an investigator giving the notice may require disclosure to be made to a technical facility or to a named technician.

4.19 Section 49 notices must describe the form and manner in which the required disclosure of information is to be made (as described in paragraph 4.17 above). Notwithstanding this, it is best practice that the person giving the notice seeks, so far as possible, to agree with the person given the notice or with their professional legal adviser the manner in which the required disclosure should take place. The conditions under which compliance with the disclosure requirement takes place must be reasonable and practicable in all circumstances.

4.20 Notices should explain clearly that it is an offence to knowingly fail to make the required disclosure (section 53 of the Act) and, where a secrecy requirement is being imposed explain the "tipping off" offence (section 54 of the Act).

4.21 Section 49 notices, including those which impose a secrecy requirement, should clarify that if the recipient has any doubt what they are required to do in response to the notice, they should contact a professional legal adviser.

Authenticity of notices

4.22 It is essential that any person who is given a notice is able to confirm its authenticity should they need to do so. Where such assurance is required the person given notice or their professional legal adviser should contact NTAC to seek confirmation that the notice is authentic and lawful. Doing so will not breach any secrecy requirement of the notice.

4.23 In practice the giving of a notice will be a stage in the progress of an investigation or operation and the person given the notice will usually have been involved earlier in that process, either as a consequence of their arrest or having been identified as being in possession of a key to the relevant information.

4.24 In addition to the statutory requirements all written notices must include a unique reference number, must identify the public authority and must provide the address of an office and a published contact telephone number using which the recipient of a notice may check its authenticity by speaking with the person who gave permission for the notice to be given or to another appropriate member of staff.

4.25 In exceptional urgent circumstances, the notice must always include contact details for the person who gave appropriate permission for the notice to be given.

4.26 Public authorities must provide a means for authenticating any notice they give at whatever time the notice is given. In addition, the person giving the notice should, when doing so in person, carry sufficient identification to confirm their office, rank or position and, if requested to do so, should produce that identification to the person being given the notice.

Description of the protected information

4.27 Persons applying for appropriate permission must ensure that their application describes the protected information which has been, or is likely to be, lawfully obtained and in relation to which a disclosure requirement is sought to be imposed as precisely as possible. Where appropriate permission is granted or where a person has appropriate permission without another person's permission the consequent notice must similarly describe the protected information.

4.28 Any notice must be in sufficient detail to enable the person given notice to be clear about the protected information to which it relates and to enable identification of any, or all, keys (including any session key) which would enable the data to be put into an intelligible form. The information can be described by reference to file names, usernames, dates and times or by any other identifiers of data, storage media, software or hardware. Where a key to the protected information can be identified the identity of the key should be included in the notice.

4.29 In some cases, it may be appropriate in order to identify or to confirm the identification of the protected data to include in, attach to or accompany the notice some or all of the protected information or a copy of some or all of it.

4.30 In respect of protected information likely to be obtained it may not always be practicable to describe the information in the same detail or as precisely as information that has been obtained – although a fuller description may be provided subsequently in the form of a schedule to the original notice.

Time to comply with a notice

4.31 The time by which any notice has to be complied with must be reasonable and realistic in all the circumstances and must take into account the practical and technical requirements of undertaking the disclosure. It will vary depending on the type and extent of the disclosure required.

4.32 Any person given a notice or to be given a notice should be afforded a reasonable period of time to seek legal or technical advice before complying with it. Equally where appropriate to do so any person who will or may be given a notice should have time to take such advice before the notice is served.

4.33 Where appropriate the time period will be related to the duration of the underlying statutory power whereby the protected information has come into the possession of the public authority or is likely to do so.

4.34 In exceptional urgent circumstances it is possible that the time by which the notice is to be complied with must be curtailed. Examples of circumstances in which immediate compliance with a notice may be appropriate are:

- an immediate threat to life such that a person's life might be endangered if the period of time for compliance were not curtailed;
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given compliance with that notice will directly assist the prevention or detection of the commission of a serious crime[14] and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the period for compliance with the notice were not curtailed, or
- a credible and immediate threat to national security or a time critical or unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the period for compliance with the notice were not curtailed.

14 See Section 81(2) of the Act.

Explaining the notice

4.35 The person giving the notice should take steps to explain, as far as is practicable and necessary (and to the extent such an explanation has not been offered before the notice is given), the contents of the notice and what is required to be done to comply with it. In particular the person giving the notice must be prepared to explain:

- on what grounds the disclosure requirement is being imposed;
- what is the relevant protected information;
- what is required to be disclosed, by when and to whom;
- any requirement to disclose a key (if appropriate) with clarification that the choice of which key to disclose is open to the recipient of the notice if that key, including any relevant session key, gives access to the information or puts it into an intelligible form;
- any secrecy provision (if appropriate);
- the consequences of not complying with the notice;
- that the person given the notice is entitled to seek legal advice about the effect of the notice and the provisions of the Act, and
- how the authenticity of the notice may be confirmed.

4.36 The person given notice must be provided with a copy of the notice which they may retain.

Amending a notice

4.37 Amendment of a notice may be required and can only be undertaken in restricted circumstances which clarify or alleviate the imposition of the disclosure requirement. These are when:

- the protected information can be identified more precisely;
- the disclosure requirement can be specified more accurately;
- the time to comply with the notice can be extended;
- a secrecy requirement can be removed, or
- where the disclosure should be made to a person not specified in the original notice.

4.38 In these cases, the amendment to the notice must:

- be undertaken in writing to the person given the notice or, if not, in a manner that produces a record of the amendment which the person given the notice may retain;
- cross reference the original unique reference number;
- record the date and time of the amendment; and
- record the name or designation and the office, rank or position held by the person amending the notice (who shall be the person who gave the notice or a person who, in the same circumstances, could have given that notice).

4.39 Any amendments to a notice must reflect the considerations of necessity and proportionality upon which the original notice was given. This means the scope of a notice or the disclosure requirement it imposes can never be extended by any amendment nor can the time to comply be curtailed. In those circumstances a new notice must be given.

4.40 The grounds for which a notice is given can never be amended, nor can a secrecy requirement be imposed by amending a notice which did not contain such a requirement. Appropriate permission must be obtained to give a notice for a different purpose or to impose a secrecy requirement.

Withdrawal of a notice

4.41 The person who had the appropriate permission to give the notice or the person who gave the notice shall withdraw it if, at any time after giving the notice and before any disclosure is made, it is no longer necessary for the person given notice to comply with it or the disclosure required by the notice is no longer proportionate to what was sought to be achieved.

4.42 Withdrawal of a notice must:

- be undertaken in writing to the person given the notice or, if not, in a manner that produces a record of the notice having been withdrawn and confirms that a disclosure is no longer required;
- identify, by reference to its unique reference number, the notice being withdrawn;

- record the date and, when appropriate to do so, the time when the notice was withdrawn; and
- record the name (or designation) and the office, rank or position held by the person withdrawing the notice.

Contributions to Costs

4.43 Should any person or persons incur costs in complying with a notice an appropriate contribution towards those costs may be made by the public authority that has imposed the disclosure requirement or obtained appropriate permission to impose that requirement.

4.44 In practice, the issue of costs will be most relevant where a third party is assisting in an investigation or operation and should be dealt with in preliminary discussions between the public authority and the person to be given the notice or any person in a company or a firm who is responsible for assisting the execution of disclosure requirements imposed upon the company or firm. Such discussions should also address any costs that might be incurred preparatory to meeting a requirement which is then not imposed or is withdrawn.

Confirmation of compliance with a notice

4.45 Where a notice has been complied with, in full or as fully as practicable in all the circumstances, the person with appropriate permission for giving the notice or the person who gave the notice must provide written confirmation of that fact to the person given the notice and, where different, also to the person who has undertaken the disclosure.

4.46 Where a disclosure is required to be made other than to the person who gave the notice (for example to a technical facility or a named technician) the person to whom the disclosure is made must provide the person who gave the notice and the person making the disclosure with confirmation, in writing or in a manner that produces a record, that the notice has been, or appears to have been, complied with. Such confirmation must be provided as soon as is practicable.

Chapter 5
RULES ON THE EFFECT OF IMPOSING DISCLOSURE REQUIREMENTS

Disclosure of protected information in an intelligible form

5.1 The effect of giving a notice to a person who, at the time the notice is served, is in possession of both the protected information[15] and a means of obtaining access to the information and of disclosing it in intelligible form (using a key or keys) is that he:

- may use any key or keys in his possession to gain access to the information or to put it into an intelligible form, and
- is required to disclose the information described in the notice in an intelligible form, and
- is required to make that disclosure in accordance with the notice.

5.2 The person given notice to disclose the information in an intelligible form can nonetheless choose to disclose any key or keys giving access to the information in an intelligible form, together with any relevant details of the cryptographic or other process used to protect the information.

5.3 Voluntary disclosure of the key or keys providing access to the protected information in an intelligible form, to the person to whom disclosure of the intelligible information was required, and by the time that disclosure was required, will mean that the person given notice to disclose the information in an intelligible form shall have complied with the requirement imposed on him to do so.

5.4 Where a disclosure requirement is to be imposed upon a business or service provider in order to assist an investigation or operation, appropriate consideration must be given to minimising any

15 Possession of the protected information includes being provided with the protected information, or a copy of it, that has come into the possession of any person.

actual or possible disruption to the business or service, or any actual or possible breach of confidence, inconvenience or unfairness to the customers of the business or users of the service.

Chapter 6
SPECIAL RULES ON THE EFFECT OF IMPOSING DISCLOSURE REQUIREMENTS

Disclosure of the means to access protected information or to put it into an intelligible form

6.1 This section concerns the circumstances in which a notice can be complied with only by the disclosure of a key, in other words:

- requiring disclosure of the means to access protected information, or
- requiring disclosure of the means to put protected information into an intelligible form.

6.2 No notice shall require the disclosure of a key unless the person granting permission for the notice to be given has directed that the disclosure requirement can only be complied with by disclosure of a key, or the person giving such a notice has appropriate permission to do so or has express permission for giving such a direction.

Special circumstances requiring disclosure of a key

6.3 The Act imposes extra conditions upon requiring disclosure of a key, in addition to those for requiring the disclosure of protected information in an intelligible form.

6.4 No person able to do so shall give a direction that a disclosure requirement can be met only by disclosure of a key unless that person believes:

- that there are special circumstances of the case which mean that the purposes for which the disclosure notice is necessary would be defeated, in whole or in part, if a key was not required to be disclosed, and

- that the requirement for disclosure of a key is proportionate to what is sought to be achieved by preventing compliance with the disclosure requirement other than by disclosure of a key.

6.5 Matters to be considered in determining such proportionality include the extent and nature of any protected information (other than that to which the disclosure requirement relates) which is protected by the same key and any adverse effect that a disclosure requirement might have on a business carried on by the person on whom the requirement is imposed.

6.6 This means that the person giving a direction that a key is required to be disclosed must consider the actual or potential collateral intrusion that will or may arise from disclosure of the key and its application to specified protected information that has come into the possession of any person or is likely to do so or might do so.

6.7 Although the special circumstances for giving direction to require the disclosure of a key will vary with each case as will the proportionality of doing so, such a requirement may be appropriate where:

- trust is an issue – where there is doubt about the integrity of the person or organisation being asked to comply with a disclosure requirement, for example the person or organisation concerned is suspected of involvement in criminality or of protecting another person or persons involved in criminality;
- credibility is an issue – where a prior disclosure of protected information in an intelligible form, whether undertaken voluntarily or in supposed compliance with a notice, is demonstrably incomplete;
- timeliness is an issue – if a person or organisation has the key to protected information but cannot, for whatever reason and having been given the opportunity to do so, provide the information in an intelligible form in exceptional urgent circumstances;
- the content of the intelligible information is an issue – where the person required to make the disclosure or a person able to undertake the disclosure on their behalf might find the intelligible form of the material offensive, obscene or otherwise distressing or

it is important in the interests of justice that they do not view or be reminded of the material;

- the key itself has evidential value – where there is reasonable belief that the key may provide evidence linking a person or persons to an offence or offences, for example where a person seeks to deny responsibility for protected information in their possession but a password or pass-phrase for the key is personal to the person being served the notice or is indicative of the material it protects. In practice it will be very rare for an investigator to reasonably believe there is a single key to the protected information which has evidential value or, less likely still, that all keys to the data have that value;
- practicality is an issue – where the key is divided into split-keys and it is not practicable or possible for the holders of the split-keys, or sufficient number of them, to act together to provide access to protected information or to disclose it in an intelligible form it may be necessary to require disclosure of one or more split-keys.

6.8 Particular care must be taken when considering the imposition of a requirement to disclose a key upon a provider of financial services in view of the crucial role that protected information has in the financial services sector. No such requirement should be imposed upon any company or firm authorised by the Financial Services Authority without prior notification to the Chief Executive of the Authority or a person designated by him for that purpose. The period of notification will be reasonable in all the circumstances of any instance.

6.9 Such notification to the Financial Services Authority will include sufficient detail to enable the Authority to understand why the requirement to disclose a key is sought to be imposed. The Authority shall consider whether the proposed disclosure requirement raises any concerns for or risks to its statutory objectives of maintaining market confidence, promoting public understanding of the financial system, the protection of consumers and the reduction of financial crime. If so, the Chief Executive of the Authority or the person designated by him will inform the applicant, or a senior official of the public authority, of those concerns or risks and the applicant must reconsider the proposed disclosure requirement taking account of those concerns or risks.

Notices requiring disclosure of a key

6.10 Where a direction has been given that a notice can be complied with only by disclosure of a key, the notice must explicitly state that the person on whom the notice is served may choose which key to disclose. The only requirement is that the key is capable of either or both obtaining access to the protected information or rendering it intelligible.

6.11 Where the person given notice is able to comply with a requirement to disclose a key without disclosing all of the keys in his possession and where there are different keys, or combinations of keys, that would enable compliance with the notice, the person given notice may choose which key or combination of keys to disclose.

6.12 Where a disclosure requirement is imposed on any person by a section 49 notice and:

- that person is not in possession of the information (either because they do not have the information, have not acquired the information or cannot be given possession);
- that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form (or so disclosing it), or
- the notice states that it can only be complied with by the disclosure of a key to the information

the effect of imposing that disclosure requirement is that the person given the notice shall be required, in accordance with the notice imposing the requirement, to disclose any key to the protected information that is in his possession at a relevant time, that is the time when the notice is given or any subsequent time before the time by which the disclosure requirement has to be complied with.

6.13 Where a person has been given notice requiring that a key be disclosed, he may choose which key or keys to disclose together with any other requested relevant details of the cryptographic methods in use, including the relevant algorithm. The information given should

be sufficient to allow the person giving the notice or the person to whom disclosure is required to be made to put the protected information described in the notice into intelligible form.

6.14 The recipient of a notice may disclose an alternative key such as a 'session key' if it enables the same access or functionality as any relevant longer term key would have enabled.

6.15 No person shall be required to disclose any key or keys other than those which are sufficient to enable the protected information described in the notice to be put into intelligible form – even if the person given notice to disclose a key is in possession of more than one key to that information. This also means that where a key is held within a multiple key store, for example among a number of keys on a smart card, necessary arrangements should be made to enable the person given notice to abstract the key and disclose it using alternative storage media.

6.16 Where a person is required by a section 49 notice to make a disclosure in respect of any protected information and that person:

- has had possession of the key to the protected information but no longer has possession of it;
- would have been required by the notice to disclose the key if it had continued to be in his possession, and
- when given the notice, or within the time by which the notice must be complied with, is in possession of any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form;

the effect of the disclosure requirement is that he shall be required to disclose all such information to the person to whom he would have been required to disclose the protected information in an intelligible form or the key. In other words, to disclose anything they have that assists putting the protected information into an intelligible form.

Chapter 7
KEEPING OF RECORDS

7.1 Public authorities must retain copies of all written applications for permission to give a section 49 notice. Such applications must be available for scrutiny by the relevant independent Commissioner with a statutory oversight role.[16] Public authorities may be required to justify to the Commissioner the content of a particular application, or their general approach to, and handling of applications and giving of notices.

7.2 All public authorities must maintain a central record of all applications for appropriate permission to give notices, of approval given by NTAC, of the grant of appropriate permission, of the giving of all notices and of compliance with each notice. These records must be available for inspection by the relevant Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions.[17]

7.3 Applications for permission to give notices, records of the giving of and compliance with notices, and information disclosed as a result of any notice, either directly or by using disclosed key material, which relate to any living identifiable individual are likely to constitute personal data and, therefore, can only be processed in accordance with the provisions of the Data Protection Act 1998.

7.4 This code of practice does not affect any other statutory obligations placed on public authorities to keep records under any other enactment. For example, where applicable in England and Wales, the relevant test given in the Criminal Procedure and

16 See Section 11 of this code.

17 The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is satisfied it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates. See section 67(5) of the Act.

Investigations Act 1996 as amended and the code of practice under that Act. This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

Chapter 8
PROCEDURES FOR DEALING WITH DISCLOSED MATERIAL

Procedures for dealing with disclosed key material

8.1 The Act clearly indicates[18] that it is the duty of every person[19] whose officers or employees include persons with duties that involve the giving of section 49 notices to ensure that arrangements are in force to safeguard keys and key material obtained by the imposition of disclosure requirements.

8.2 Such persons should ensure necessary arrangements are in force:

- that any disclosed key is used only for obtaining access to, or putting into intelligible form, protected information described in the notice as a result of which the key was disclosed (or could have been described in such a notice had the key not already been disclosed);
- that the use of any disclosed key is reasonable with regard both to the uses to which the person with the key is entitled to put any protected information to which the key relates and to the other circumstances of the case (in other words only reasonable use may be made of any disclosed key);
- that the use of and retention of any disclosed key is proportionate to what is sought by its use or retention, and where any key is retained, its retention must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid (otherwise it should be destroyed);

18 Section 55 of the Act.

19 In particular the Secretary of State and every other Minister of the Crown in charge of a government department, every chief officer of police, the Director General of the Serious Organised Crime Agency and the Commissioners of Revenue and Customs.

- that the number of persons to whom any disclosed key is made available and the number of copies made of the key, if any, are each limited to the minimum necessary for the purpose of putting the protected information in an intelligible form;
- that any disclosed key is stored, for as long as it is retained, in a secure manner. The appropriate level of security for any disclosed key should be proportionate to its intrinsic or financial value or to the sensitivity of the information protected by the key, and should at least correspond to its security before disclosure;
- that all physical key material no longer required to be retained is returned to the person who disclosed it;
- that all records of any disclosed key are destroyed permanently as soon as the key is no longer required for the purpose of enabling protected information to be put into an intelligible form.[20]

8.3 Such arrangements shall be recorded in writing setting out internal procedures for the disclosure, copying, storage and destruction of any disclosed key material, which minimise the availability of disclosed key material, and shall be agreed with the appropriate Commissioner.

8.4 Extra care and security should be afforded to a key (a 'multi-use key') that has been used to protect information in addition to the protected information in the possession of the public authority or likely to come into its possession. Even though a person given notice is able to choose which key to disclose, they may disclose a multi-use key. The person to whom disclosure is made should ensure that if a multi-use key is disclosed he is aware of that and can protect the key appropriately.

8.5 Key material must be stored in a *physically* secure way such that it cannot be accessed through any means other than physically. For example the use of a floppy disk or USB stick may be appropriate but a laptop would not as it could theoretically be accessed remotely.

20 See paragraph 8.10

8.6 Data should be secured behind an appropriate number of security zones using, where possible, different methods of security. For example material requiring the highest level of security should be stored in a combination safe, inside a locked store in an access controlled office which itself is within a 24 hour guarded building. Access to the data should not be possible by one person acting alone, requiring at least two people to have to conspire to unlawfully use any key. For example the combination to a safe in a locked store should not be known by a key holder of the store.

8.7 Where keys or copies of keys are made available to a person other than the person to whom the key was disclosed a full audit trail must be maintained and be available for inspection by the appropriate Commissioner.

8.8 The number of persons to whom the detail of any key or the fact of possession of a disclosed key is made available must be limited to the absolute minimum necessary to allow protected information to be made intelligible.

8.9 Neither the key, the detail of any key, nor the fact of possession of a key may be disclosed to any person unless that person's duties are such that he needs to know the information to carry out his duties. This obligation applies equally to disclosure to additional persons within an agency or public authority, to disclosure outside the agency or public authority and to any data processing facility.

8.10 Under normal circumstances where protected information is put into an intelligible form using a disclosed key, and that intelligible information is used in evidence or is disclosed in criminal proceedings, copies of the key will similarly be required for evidential or disclosure purposes (notwithstanding any necessary public interest immunity).

8.11 Where a requirement for disclosure of a key is necessary in relation to protected information obtained in exercise of a statutory power, that key will be handled with the due care and attention required for any sensitive or valuable evidential material. It shall be the duty of the person to whom the key is disclosed or the official in

charge of any processing facility to afford it a higher level of security if that is necessary in the particular circumstances of the case and to protect the key material from unauthorised disclosure.

Procedures for dealing with disclosed intelligible material

8.12 Intelligible information which is disclosed in compliance with a notice should be handled with the same care and attention as other material that has been obtained by means of a statutory power to seize or otherwise require the production of documents or other property. Any loss or damage incurred by a relevant person (within the meaning in section 55(5) of the Act) arising from any failure to safeguard disclosed intelligible information may give rise to a civil action against the public authority or the person responsible for that failure.

Damages

8.13 Should any person who has made a disclosure having been given a section 49 notice or whose own protected information or whose own key has been disclosed as a consequence of a notice incur any loss or damage in consequence of:

- any breach by a person on whom the duties to safeguard disclosed keys apply, or
- any contravention of the arrangements for those safeguards made by any person who is under the control of a person to whom section 55 of the Act applies;

the injured person may take civil action in relation to such a breach or contravention against the person on whom the duties to safeguard disclosed keys apply.

8.14 Any court hearing such proceedings shall have regard to any opinion with respect to the matters to which the proceedings relate that is or has been given by a relevant Commissioner.

Chapter 9
APPROPRIATE PERMISSION FOR THE GIVING OF NOTICES

9.1 Any person using the powers in Part III, and specifically any person giving a section 49 notice, must have appropriate permission to do so. Circumstances in which appropriate permission may be granted or persons have the appropriate permission are described in Schedule 2 to the Act.

9.2 In general the permission to give a notice must be given by a person with at least the same level of authority as that required for the exercise of any power to obtain the protected information. With certain exceptions, the appropriate permission to give a notice should, so far as is practical, be given by the same person authorising, or who authorised, the use of any power to obtain the protected information.

9.3 No person can seek to obtain appropriate permission to give a notice without the approval of NTAC to do so. Persons able to grant appropriate permission for the giving of notices must ensure that the approval of NTAC has been obtained before granting appropriate permission.

9.4 Appropriate permission can never be given for a notice in respect of protected information that has been obtained unlawfully by a public authority.

Appropriate permission granted by a judicial authority

9.5 Public authorities may always seek appropriate permission for giving a section 49 notice from a judicial authority. Any member of a public authority will have appropriate permission if, and only if, written permission for giving the notice has been granted by:

- a Circuit judge, in England and Wales;
- a sheriff, in Scotland; or
- a county court judge, in Northern Ireland

9.6 Where such a judicial authority has granted appropriate permission to give a section 49 notice, no further permission from any other person is required.

9.7 Where protected information has been obtained under statute but without a warrant (other than by the police, HMRC, SOCA or a member of HM forces) a person shall not have the appropriate permission, even where permission is granted by a judicial authority, unless:

- he is the person who exercised the statutory power to obtain the protected information (or is a person who could have exercised it); or
- he is the person to whom the protected information was provided or disclosed (or is a person to whom provision or disclosure of the information would have discharged the statutory duty); or
- he is or is likely to be such a person when the power is exercised or the protected information provided or disclosed.

Appropriate permission granted by a person holding judicial office

9.8 Public authorities may obtain appropriate permission for giving a section 49 notice from persons holding judicial office where protected information is likely to be, or has been, obtained under a warrant issued by such a person holding judicial office, that is to say:

- any judge of the Crown Court or of the High Court of Justice;
- any sheriff;
- any justice of the peace;
- any resident magistrate in Northern Ireland; or
- any person holding any such judicial office as entitles him to exercise the jurisdiction of a judge of the Crown Court or of a justice of the peace.

9.9 Appropriate permission may be given by the person who issues or issued the warrant or by a person holding judicial office who would have been entitled to issue the warrant. Such permission might be granted, for example, in relation to a search warrant or production order under the Police and Criminal Evidence Act 1984 as amended or the Drug Trafficking Act 1994 as amended.

9.10 Any person will have appropriate permission if:

- before protected information is obtained, the warrant contained explicit permission for giving section 49 notices in relation to protected information to be obtained under the warrant or,
- subsequent to the issue of the warrant, written permission is granted for giving section 49 notices in relation to protected information obtained under the warrant.

9.11 Only a person who was entitled to exercise the power conferred by the warrant or who is a person on whom the power conferred by the warrant was, or could have been, conferred may have appropriate permission to give a notice in relation to protected information obtained, or to be obtained, under a warrant issued by a person holding judicial office. In other words, a person only has appropriate permission if that person could execute, has executed or could have executed the warrant,

9.12 Where protected information is obtained under a statutory power without a warrant in the course of, or in connection with, the execution of a warrant containing appropriate permission, or where material unconnected with a search warrant is lawfully seized, for example under section 19 of the Police and Criminal Evidence Act 1984 ('PACE'), appropriate permission for giving a notice in respect of that additional information will be required.

Appropriate permission granted by the Secretary of State

9.13 Where protected information is likely to be, or has been, obtained under a warrant issued by the Secretary of State (for example an interception warrant under section 8 of the Act, or a warrant for interference with wireless telegraphy, entry or interference with property under section 5 of the Intelligence Services Act 1994) appropriate permission for giving a section 49 notice in respect of that information may be obtained from the Secretary of State.

9.14 Only persons holding office under the Crown, the police, a member of staff of the SOCA or HMRC may have the appropriate permission in relation to protected information obtained, or to be obtained, under a warrant issued by the Secretary of State.

9.15 Such persons have appropriate permission if the warrant issued by the Secretary of State contains permission for giving section 49 notices in relation to protected information to be obtained under the warrant or, subsequent to the issue of the warrant, the Secretary of State grants written permission for giving section 49 notices in relation to protected information obtained under the warrant.

9.16 The Secretary of State may also grant written permission for giving section 49 notices where protected information has come, or is likely to come, into the possession of any of the intelligence services without a warrant or where protected information has been, or is likely to be, obtained lawfully by any of the intelligence services using a statutory power but without the exercise of a warrant[21] or where protected information is in the possession of any of the intelligence services, or is likely to come into their possession, for example material voluntarily disclosed or provided to any of the intelligence services.[22]

9.17 Where the Secretary of State's permission is sought he must grant the permission personally in writing or, in an urgent case, expressly authorise the grant of permission in which case a senior official may sign it.[23]

Appropriate permission granted by an authorising officer

9.18 Where protected information is likely to be, or has been, obtained in consequence of an authorisation under Part III of the Police Act 1997 (authorisation of otherwise unlawful action in respect of property) appropriate permission for giving a section 49 notice may be obtained from an authorising officer within the meaning of section 93 of the 1997 Act or, in urgent cases, section 94 of that Act.

9.19 Any person will have appropriate permission if, before protected information is obtained, the authorisation given under the 1997 Act contained permission for giving notices in relation to protected information to be obtained under the authorisation or, subsequent to

21 See paragraph 3 of Schedule 2 to the Act.

22 See paragraph 5(2) of Schedule 2 to the Act.

23 See paragraph 8 of Schedule 2 to the Act.

the issue of the authorisation, written permission is granted for giving notices in relation to protected information obtained under the authorisation.

9.20 Only the police, SOCA and HM Revenue and Customs may have the appropriate permission in relation to protected information obtained, or to be obtained, under an authorisation under Part III of the Police Act 1997.

Appropriate permission granted by a person exercising a statutory function

9.21 The police, SOCA, HMRC and members of HM forces have appropriate permission, without requirement for permission to be granted by a judicial authority, in relation to protected information:

- that is likely to be, or has been, obtained by the exercise of a statutory power (and is not information obtained under a warrant issued by the Secretary of State or a person holding judicial office, or an authorisation under Part III of the Police Act 1997, or information obtained by the intelligence services), for example material obtained by the police under section 19 of PACE;
- that is likely to be provided or disclosed, or has been provided or disclosed, in pursuance of a statutory duty;
- that is likely to come into possession of, or is in the possession of, the police, SOCA, HMRC or a member of HM forces under statute.

9.22 In these circumstances, if a section 49 notice is to require disclosure, such permission may be given in line with the general requirements relating to appropriate permission.

General requirements relating to appropriate permission

9.23 Paragraph 6 of Schedule 2 to the Act sets out general requirements relating to persons having appropriate permission in the police, SOCA, HMRC or who are members of HM forces. A person has appropriate permission in relation to any protected information if he has possession of the protected information, or is likely to have possession of it, or is authorised to act on behalf of such a person.

9.24 Where protected information has come into the possession of the police by means of the exercise of powers conferred by section 44 of the Terrorism Act 2000 (power to stop and search), the appropriate permission to give a section 49 notice in relation to that information must be granted by an officer holding at least the rank of Assistant Chief Constable of a police force or the rank of Commander in the Metropolitan Police Service or the City of London Police.

9.25 Where protected information has come into the possession of the police, SOCA, HMRC or a member of HM forces, a person shall not have appropriate permission unless that person holds certain rank or designation:

- Police – Superintendent or above;
- SOCA – Director General or a member of staff of the SOCA of or above such level as the Director General may designate for this purpose;
- HMRC – the Commissioners for Revenue and Customs themselves or an officer of their department of or above such level as they may designate for this purpose;
- HM forces – Lieutenant Colonel or its equivalent or above

Appropriate additional permission for giving directions for the disclosure of keys

9.26 Where a disclosure requirement can only be met by disclosure of a key, appropriate additional permission for giving such a direction is required in the following circumstances:

- for a direction by any constable (except a constable who is a member of the staff of the SOCA), and a member of Her Majesty's forces who is a member of the police, by or with the permission of a chief officer of police;
- for a direction by SOCA, by or with the permission of the Director General of the SOCA;
- for a direction by HMRC, by or with the permission of the Commissioners for Her Majesty's Revenue and Customs;

- for a direction by a member of Her Majesty's forces who is not a member of the police force, by or with the permission of, or above, the rank of Brigadier (or equivalent).

9.27 Any permission granted for giving a direction that a disclosure requirement can only be met by disclosure of a key must be given expressly in relation to the specific direction.

9.28 Any direction to disclose a key given by or with the permission of a chief officer of police, the Director General of the SOCA or the Commissioners for Her Majesty's Revenue and Customs must be notified to the Chief Surveillance Commissioner.

9.29 Any direction to disclose a key given by a member of Her Majesty's forces shall also be notified to the Chief Surveillance Commissioner except where the direction is given by a member of Her Majesty's forces who is not a member of a police force and is in connection with Her Majesty's forces other than those in Northern Ireland in which case notification must be given to the Intelligence Services Commissioner.

9.30 Notification to the appropriate Commissioner of any direction to disclose a key must be given in writing or electronically as soon as practicable and within no more than 5 working days of the direction being given. Failure to do so will constitute a breach of this code.

Duration of appropriate permission

9.31 Permission granted to any person to give a section 49 notice can cease to have effect.

9.32 All persons who grant permission for the giving of notices must attach an appropriate duration to all such permissions. Permission lasting for a lengthy period will always need careful ongoing consideration particularly with regard to whether in the specific circumstances the notice remains necessary and proportionate.

9.33 Permission, once granted, has effect – regardless of the cancellation, expiry or discharge of any warrant or authorisation in which that permission is contained or to which it relates – until such time, if any, as that permission:

- expires in accordance with the limitation on its duration that was contained in the terms of the permission, or
- is withdrawn by the person who granted the permission or by a person holding any office or other position that would have entitled that person to grant the permission.

Chapter 10
OFFENCES

10.1 The Act provides for two criminal offences: failure to comply with a notice (Section 53) and making an unauthorised disclosure (tipping-off) (Section 54).

Failure to comply with a notice

10.2 Where a person given a section 49 notice knowingly fails to make the disclosure required they commit an offence. If the disclosure required is necessary in the interests of national security they may be convicted on indictment to a maximum of 5 years imprisonment[24] or in any other case 2 years. On summary conviction they may be liable to a maximum six-month term of imprisonment or a fine not exceeding the statutory maximum or both.

10.3 In proceedings against any person for failing to comply with a notice, if it is shown beyond a reasonable doubt that he was in possession of a key to the protected information at any time before the notice was given, that person shall be considered to be in possession of that key at all subsequent times unless it is shown that the key was not in his possession after the giving of the notice and before the time that he was required to disclose it.

10.4 If the person fails to raise some doubt as to whether he had the key when the notice was given or before any subsequent time by which he was required to make the disclosure, that person shall be taken to have continued to be in possession of that key.

24 Section 53 as amended by Section 15, Terrorism Act 2006

10.5 A person shall be taken to have shown they were not in possession of a key to protected information at a particular time if sufficient evidence of that fact is adduced to raise an issue with respect to their not having had possession of the key. The prosecutor has to prove the contrary beyond reasonable doubt.

10.6 It is a defence for a person to show it was not reasonably practicable to make the disclosure required within the time limit given in the notice, for example for purely technical reasons, but that the disclosure was made as soon afterwards as was reasonably practicable.

10.7 A person shall have failed to comply with a notice where a disclosure is made and it is shown beyond a reasonable doubt that the disclosure made is not in compliance with the notice given, for example the information put into intelligible form is demonstrably partial, incomplete or information other than the protected information described in the notice.

Tipping off

10.8 Section 49 notices may contain a provision requiring the person to whom the notice is given and every other person who is permitted to or who necessarily becomes aware of it or of its contents to keep secret the giving of the notice, its contents and the things done to comply with it. The inclusion of a secrecy requirement in a notice requires the consent of the person granting permission for the notice to be given or for the person giving the notice to have that permission.

10.9 This secrecy requirement is designed to preserve – but only where necessary – the covert nature of an investigation and to deter deliberate and intentional behaviour designed to frustrate statutory procedures and assist others to evade detection.

10.10 The circumstances in which a secrecy requirement may be imposed are restricted in section 54 of the Act. There are two conditions;

- the first condition is that the protected information has come, or is likely to come, into the possession of the police, SOCA, HMRC or the intelligence services;

- the second condition is that the means by which the information was obtained needs to be kept secret in order to maintain the effectiveness of an investigation or operation or of investigative techniques generally, or in the interests of the safety or well being of any person.

10.11 Public authorities other than those specified in section 54 may not include a secrecy requirement in their disclosure notices.

10.12 In imposing any secrecy requirement it is enough for any person giving consent for that requirement or giving a notice including such a requirement to have considered that there is a particular person from whom it is reasonable to withhold the information.

10.13 Where a secrecy requirement is imposed, the notice must make this clear and the person given notice and any other person who needs to know about the notice should be made aware explicitly of that requirement. The notice should also inform the recipient that he may nonetheless approach a professional legal adviser for advice about the effect of the provisions of Part III of the Act and that he may revoke any key that is disclosed provided the underlying reason for its revocation is not disclosed.

10.14 The tipping-off offence is committed by a person who makes a disclosure to any other person of anything that he is required by the section 49 notice to keep secret.

10.15 A notice containing a secrecy requirement can never be imposed upon a vulnerable person or a child.

Automatic tipping-off

10.16 For security purposes, certain software has been designed to give an automatic warning when a key has been disclosed or has ceased to be secure. This can conflict with a secrecy requirement, although the person seeking permission to give the notice should, so far as is practicable, establish whether the intended recipient of the notice uses such software and if so what reasonable steps they can take to prevent or defer such disclosure.

10.17 Where a disclosure occurs contrary to a secrecy requirement it is a defence for a person to show that the disclosure was automatic and effected entirely by software designed to indicate that a key to protected information has ceased to be secure and they could not reasonably have prevented that taking place, whether after being given the notice or becoming aware of it or its contents.

10.18 It is also a defence for a person to show that the disclosure was made by or to a professional legal adviser as part of giving advice to a client of his about the effect of the provisions of Part III of the Act and that the person to whom or by whom the disclosure was made was the client or a representative of the client; or where a disclosure was made by a legal adviser in connection with any proceedings before a court or tribunal.

10.19 If a disclosure is made by or to a professional legal adviser with a view to furthering any criminal purpose that disclosure shall not be a defence in proceedings for a Section 54 offence.

Authorised disclosure

10.20 It is not the intention of the Act to penalise individuals within organisations who, for example, have been given a notice imposing a secrecy requirement but need the assistance of another colleague in order to comply with the notice. That other person must be made aware of the secrecy requirement. Should proceedings be brought for an unlawful disclosure in respect of the notice it is a defence for a person other than the person to whom the notice was given to show that he neither knew nor had reason to suspect the notice contained a secrecy requirement.

10.21 In section 54(9) the Act provides a statutory defence to unauthorised disclosure where the disclosure was made to a relevant Commissioner or was authorised by a Commissioner; by the terms of the notice; by, or on behalf of, the person who gave the notice or by, or on behalf of, a person in lawful possession of the protected information to which the notice relates.

Chapter 11
OVERSIGHT

11.1 The Act provides for Commissioners whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained in Part III – except where those powers and duties are being exercised by a judicial authority.

11.2 There are three independent Commissioners with relevant oversight responsibilities:

- **the Interception of Communications Commissioner** who keeps under review:
  - the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under Part III, particularly the grant of appropriate permission for the giving of a section 49 notice in relation to information obtained under Part I (intercepted material and other related communications data), and
  - the adequacy of the arrangements for complying with the safeguards in section 55 in relation to key material for protected information obtained under Part I.
- **the Intelligence Services Commissioner** who keeps under review (so far as they are not required to be kept under review by the Interception of Communications Commissioner):
  - the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by Part III particularly the grant of appropriate permission for the giving of a section 49 notice in connection with, or in relation to, the activities of the intelligence services and the activities (other than activities in Northern Ireland) of the Ministry of Defence ('MOD') and members of HM forces;

  - the exercise and performance by members of the intelligence services of the powers and duties conferred or imposed on them by or under Part III;
  - the exercise and performance, in places other than Northern Ireland, by officials of the MOD and members of HM forces of the powers and duties conferred or imposed on such officials or members of HM forces by or under Part III, and
  - the adequacy of the arrangements for complying with the safeguards in section 55 in relation to members of the intelligence services and, in connection with any of their activities in places other than Northern Ireland, in relation to officials of the MOD and members of HM forces.
- **the Chief Surveillance Commissioner** who keeps under review, so far as they are not kept under review by the other Commissioners:
  - the exercise and performance, by any person (other than a judicial authority or a person holding judicial office) of the powers and duties conferred or imposed, otherwise than with the permission of a judicial authority or a person holding judicial office, by or under Part III, and
  - the adequacy of the arrangements for complying with the safeguards in section 55 by those persons whose conduct is subject to review by the Chief Surveillance Commissioner.

11.3 This code does not cover the exercise of the Commissioners' functions. It is the duty of any person who uses the powers conferred by Part III, or on whom duties are conferred, to comply with any request made by a Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

11.4 Should any Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a public authority exercising or complying with the powers and duties under Part III of the Act he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him to effectively engage the Tribunal.

Chapter 12
COMPLAINTS

12.1 The Act established an independent Tribunal ('the Investigatory Powers Tribunal'). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction, which includes the giving of a notice under section 49 or any disclosure or use of a key to protected information.

12.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedures can be obtained from the following address:

The Investigatory Powers Tribunal,
PO Box 33220
London
SW1H 9ZQ
☎ 020 7035 3711

Notes

Notes

This code of practice relates to the powers and duties conferred or imposed under Part 3 of the Regulation of Investigatory Powers Act 2000 to require the disclosure of protected electronic information (electronic data) in an intelligible form or to acquire the means by which protected electronic information may be accessed or put in an intelligible form. It provides important guidance on the scope of the powers, on the role of the National Technical Assistance Centre as the lead authority in all matters relating to Part 3 and on the imposition of disclosure requirements, particularly those where a key to protected informed is required to be disclosed.

This code is aimed at members of public authorities who are involved in the investigation of protected electronic information, and those with permission to authorise the imposition of disclosure requirements, and to persons upon whom a duty may be imposed under Part 3.

£7

TSO
information & publishing solutions

www.tso.co.uk

ISBN 978-1-84726-202-8

9 781847 262028