INVESTIGATION OF ELECTRONIC DATA PROTECTED BY ENCRYPTION ETC

DRAFT CODE OF PRACTICE

Preliminary draft code: This document is circulated by the Home Office in advance of enactment of the RIP Bill as an indication of current thinking. It will be subject to changes and additions. This circulation is not the publication referred to in clause 69(3) of the Bill, which can only take place after enactment. This Is a preliminary draft on which comments are welcomed. Further, informal consultation will be required before the formal consultation process begins under clause 69(3) of the Bill.

This document contains the original text of the Home Office Code of Practice for Part III of the RIP Bill with annotations in blue italic text.

The conclusions are that:

(a) no new information is provided on the situations in which keys can be seized;

(b) the security interests of key owners are almost completely ignored – it appears that some types of key – for example, passwords and PINs – will not be given any formal security protection when seized;

(c) there are no specifications (or even coverage) of the design, development, implementation and operation of the procedures, standards and technical approaches that are needed for the protection of keys or information obtained using RIP powers;

(d) issues concerning the misuse of seized keys or information (other than privileged information) – for example, disciplinary actions – are not covered at all.

Far from allaying fears about key protection, this document confirms that keys will be at risk if seized.

Fears about the impact of this Bill on trust and confidence in the provision of Internet security services are well founded. The UK's e-commerce aspirations are now at risk.

FOREWORD

Part III of the Regulation of Investigatory Powers Act 2000 provides powers to help deal with the use by criminals of cryptographic and other information security technologies.

In very simple terms, cryptography is the art or science of securing data or communications. The technology is good for individuals' privacy and is a vital component in making e-commerce work successfully. Cryptography can, for example, help instil trust in doing business over the Internet. This is because the technology offers the following services:

- **integrity** (guaranteeing that data has not been accidentally or deliberately corrupted);

- **authentication** (guaranteeing that the originator or recipient of material is the person they claim to be); and

- **confidentiality** (protecting a message to ensure that its contents cannot be read by anyone other than the intended recipient).

The difficulty is that the very same technologies, which are good for business and individual privacy, also present new opportunities for criminals. Here it is the confidentiality aspect that is important - the ability of criminals to protect or "encrypt" the content of their communications (such as emails) or stored data (their computer disks for example). Relevant statutes (e.g. the Police and Criminal Evidence Act 1984) were enacted before the emergence of the Internet as a mass communications medium and the wider public availability of strong encryption. The measures in Part Ill of the Regulation of Investigatory Powers Act 2000 seek to help ensure that the effectiveness of existing powers are not undermined as the technology concerned becomes more readily available and easier to use.

There is very little evidence to show that encryption is hindering Law Enforcement authorities at the moment. This is more a fear of what might happen rather than a careful assessment of what is likely to occur. The arguments used in support of these proposals could equally be used to suggest that, because criminals sometimes meet in each other's houses, all citizens should be required to have closed circuit televisions fitted in their homes with connections to local police stations in case the police want to know what is happening.

In countering criminal misuse of the Internet, it is vital to act on careful assessment of what is likely to happen rather than on fear alone. It is also important to consider all the options for countering criminal misuse so that the most realistic and effective ways of detecting and preventing crime are implemented. This legislation fails to meet these requirements but undermines the rights of honest citizens by creating uncertainties about Internet security provision. These measures will be technically ineffective but, worse than this, they could easily create a false sense of confidence in law enforcement circles that will undermine investment in the more effective approaches that are now vital in protecting society from Internet criminals.

CONTENTS

Section 1 : GENERAL

Section 2 : POWER TO REQUIRE DISCLOSURE

Section 3 : PERMISSION LEVELS

Section 4 : PROCESS OF GIVING PERMISSION

Section 5 : FORM OF NOTICES

Section 6 : SERVICE OF NOTICES

Section 7 : EFFECT OF SERVING A NOTICE

Section 8 : KEYS

Section 9 : SECRECY REQUIREMENT AND "TIPPING OFF"

Section 10 : RECEIPT OF INFORMATION

Section 11 : SAFEGUARDS

Section 12 : OVERSIGHT

Section 13 : COMPLAINTS

Appendix 1 : Specimen section 47 notice

Appendix 2 : Specimen section 47 notice requiring key disclosure

1 GENERAL

Extent and Availability

1.1 This code of practice provides guidance for public authorities on use of the powers concerning the investigation of electronic data protected by encryption provided for under Part Ill of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). Powers concerning interception of communications, collection of communications data, use of intrusive and directed surveillance and covert human intelligence sources under Parts I and II of the 2000 Act are dealt with in separate codes of practice.

1.2 The measures in Part Ill of the 2000 Act are ancillary to other statutory and non-statutory powers and functions of public authorities. This code must therefore be read in conjunction with other relevant codes of practice (e.g. that covering the powers contained in Part I of the 2000 Act).

1.3 A copy of this code should be readily available, for reference purposes, at public offices of public authorities who may obtain a permission to serve disclosure notices under the powers contained in Part Ill of the 2000 Act and should be readily available for consultation and reference by all members of public authorities who may seek such permissions. It should also be available where people are detained in custody.

1.4 The 2000 Act provides that the code is admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, it must be taken into account.

Overview

1.5 Part Ill of the 2000 Act establishes a power to require any person served with an appropriate notice to disclose protected (e.g. encrypted) information in an intelligible form ("plain text"). The Part Ill power is ancillary to all statutory and non-statutory powers and functions of public authorities. Its use by any public authority requires proper and specific permission. A number of statutory requirements must be met before any such permission can be given to exercise the disclosure power. There are extra requirements where a decryption key - rather than plain text - is desired. The 2000 Act sets out statutory safeguards for the protection of all information obtained under the Part Ill power. There are associated offences. The Act also provides for independent oversight of the measures in Part Ill and an independent complaints mechanism.

2 POWER TO REQUIRE DISCLOSURE

2.1 This section describes the circumstances in which a public authority may seek permission to serve a section 47 notice.

2.2 Part Ill of the 2000 Act does not provide any new powers to allow a public authority to obtain information which it cannot already obtain. The provisions are ancillary to existing statutory or non-statutory powers and functions. Permission to serve a disclosure notice may only be given in respect of lawfully obtained information which has been, or is likely to be, protected in some way (e.g. it has been encrypted).

2.3 Section 47(1) of the 2000 Act sets out the circumstances when the power to serve a disclosure notice may apply. It does so by describing the various means by which protected information may be lawfully obtained by publicauthorities. By way of illustration, this includes information which has been, or is likely to be:

- seized under a judicial warrant;
- disclosed under a judicial production order;
- intercepted under a warrant personally authorised by the Secretary of State;
- obtained under an authorisation given under Part II of the Regulation of Investigatory Powers Act 2000;
- obtained by a public authority under their statutory functions but not under a warrant;
- or has, or is likely to, come lawfully into the possession of a public authority but not by use of their statutory functions.

2.4 So a public authority may seek permission to serve a disclosure notice where protected information is already in their possession. But the 2000 Act also contains a forward looking element in section 47(1) such that a public authority may, for example, apply for permission to same a disclosure notice at the same time as an application is made to use the underlying power to obtain information. In such cases, it must be likely that encryption is being used to protect information. The authority concerned must explain this fully in making the case for permission to serve a notice as described in Section 4 of this code (Process of giving permission).

2.5 Permission to serve a disclosure notice may not be given where any protected information has been obtained unlawfully by a public authority.

3 PERMISSION LEVELS

3.1 This section explains the level of permission needed to serve a section 47 notice.

3.2 The appropriate level of permission required to same a disclosure notice will vary according to the public authority involved and to the power under which

protected material has been, or is likely to be, lawfully obtained in a particular instance. The details of these levels are contained in Schedule 2 to the 2000 Act.

3.3 The general principle is that permission to serve a disclosure notice must be given by at least the same level of authority as required for the exercise of the underlying power. And, with certain exceptions, the general practice will be that permission to same a notice should be given by the same person who authorised the use of the underlying power (where applicable).

3.4 In more detail, permission to serve a disclosure notice may be obtained by public authorities in the manner set out below.

Judicial permission

Circuit judge

3.5 Firstly, by virtue of paragraph 1 of Schedule 2 to the 2000 Act, public authorities may always seek permission to serve a disclosure notice from:

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

3.6 If permission has been granted by any of the above, no further permission from any other person is required in order to serve a disclosure notice.

3.7 For public authorities not empowered by Secretary of State warrant or otherwise specifically named in Part Ill of the 2000 Act[1], permission to serve a disclosure notice must always be obtained from a Circuit judge in England and Wales, a sheriff in Scotland or a county court judge in Northern Ireland by virtue of paragraph 4(3) and (4) of Schedule 2 to the Act.

Other judicial figures

3.8 Paragraph 2 to the 2000 Act describes other cases in which public authorities may obtain judicial permission to serve a disclosure notice. These are where protected information has been, or is likely to be, obtained under a statutory warrant issued judicially. In those circumstances, a judicial officeholder who could have issued the warrant may also grant permission to serve a section 47 notice. The judicial office-holders to whom this applies are:

- any judge of the Crown Court or of the High Court of Justiciary;

[1] This means public authorities other than the police, HM Customs and Excise, HM Forces and the security and intelligence agencies (Security Service, SIS, GCHQ).

- 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.

Secretary of State permission

3.9 Where protected information has been, or is likely to be, obtained under a warrant authorised personally by the Secretary of State (e.g. an interception warrant under Part I of the 2000 Act, permission to serve an associated disclosure notice may be obtained from the Secretary of State by virtue of paragraph 2 to Schedule 2 to the 2000 Act.

3.10 Only persons holding office under the Crown, the police and HM Customs and Excise may obtain permission to serve a notice in these circumstances.

3.11 By virtue of paragraphs 3 and 5 of Schedule 2 to the 2000 Act, permission to serve a disclosure notice may also be obtained from the Secretary of State where protected material has been, or is likely to be, lawfully obtained by the security and intelligence agencies (Security Service, SIS, GCHQ) under their statutory powers but without a warrant or where protected information has been or is likely to be, obtained lawfully by these agencies without the exercise of statutory powers.

3.12 Where the Secretary of State's permission is needed, this means his personal permission (by virtue of paragraph 8 of Schedule 2 to the Act). He must sign the permission, except in an urgent case, where he must expressly authorise the permission but where it may be signed by a senior official.

Where information is of a character where it could be intercepted or it could be obtained as stored computer data – for example, electronic mail – it may well be much easier for a new disclosure notice to be issued for both the protected information and the key in their 'stored data' forms. This would circumvent the intention that the Secretary of State should approve a disclosure notice for intercepted information.

Other permissions

Police Act 1997

3.13 This paragraph applies only to the police and HM Customs and Excise. Where protected material is, or is likely to be, obtained under an authorisation given under Part Ill of the Police Act 1997, permission to serve an associated disclosure notice may be obtained from an authorising officer as defined in section 93 (and 94) of that Act[2].

[2] By way of illustration this means, for example, Chief Constable, Director General NCIS etc.

Police, HMC&E and HM Forces

3.14 This paragraph applies only to the police, HM Customs and Excise and HM Forces. Where protected material is, or is likely to be, obtained under statutory powers but without a warrant; provided, disclosed or otherwise lawfully in the possession of the public authority concerned, permission to serve a relevant disclosure notice may be given by a person within the particular authority concerned, without requiring a permission as set out in paragraph 3.5 of this code. But such permission may only be given at the following levels:

- Police - superintendent or above;
- HMC&E - by the Commissioners for Customs and Excise themselves or by an officer of their department of or above such level as they may designate for this purpose;
- HM Forces - lieutenant colonel or above.

3.15 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); or
- Section 13A or 13B of the Prevention of Terrorism (Temporary Provisions) Act 1989;

permission to serve a disclosure notice may be given by persons of or above the ranks set out in the relevant provisions of those Acts.[3]

4 PROCESS OF GIVING PERMISSION

4.1 This section concerns the process of giving permission for a section 47 notice to be served. Normally, notices will require the disclosure of protected information in an intelligible form (plain text).

4.2 Extra tests apply where a key itself - rather than simply the plain text - is being sought. The details are set out in Section 8 of this code (Keys). Details of the circumstances when a notice may contain a secrecy requirement are set out in Section 9 of this code.

Who may apply

4.3 As set out in Section 2 of this Code, the disclosure power contained in Part Ill of the 2000 Act is ancillary to all statutory and non-statutory powers and functions. It follows that any public authority which may, for example, lawfully seek to intercept, or

[3] e.g. Commanders of the Metropolitan Police.

to obtain or require the disclosure of information, may apply to the appropriate person (as detailed in Section 3 of this code) for permission to serve a disclosure notice where they can satisfy the requirements set out below.

Application process

4.4 Persons with the appropriate authority will decide whether to give permission for a disclosure notice to be served in an individual case.

4.5 Public authorities may seek permission to serve a disclosure notice in relation to protected information that has already been obtained under some lawful authority. To do so, the public authority concerned must make out the case for serving a notice as outlined in paragraph 4.6 below. But as described in section 2 of this code, Part III of the 2000 Act also provides a forward looking element to enable a public authority to seek permission to serve a disclosure notice in relation to protected material which is not yet in their possession. Where this can be justified, public authorities may seek permission to same a disclosure notice at the same lime as making an application to use the power under which protected information is to be lawfully obtained.

4.6 Except where urgency makes this impossible, applications for permission to serve a disclosure notice should be in writing. They should contain the following minimum information:

- background to the case;
- a description of the protected information which has been, or is likely to be, lawfully obtained;
- confirmation of the manner in which this information has been, or is likely to be, lawfully obtained;
- an explanation of why it is believed that the person on whom it is intended to serve a disclosure notice has possession[4] 4 of a key to the particular protected information described in the application;
- justification for why it is believed that imposing a disclosure requirement is necessary whether:

[4] Section 54(2) of the 2000 Act states that references to a persons having information (including a key to protected information) in his possession include references-

(a) to its being In the possession of a person who is under his control so far as that information is concerned;
(b) to his having an Immediate right of access to it or an immediate right to have it transmitted or employee supplied to him; and
(c) to its being, or being contained in, anything which he or a a person under his control is entitled, in exercise of any statutory power and without otherwise taking possession of it to detain inspect or search.

- 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
- likely to be of value in carrying out the statutory powers or duties of the public authority making the application (the precise power or duty being identified);

- a consideration of the proportionality implications of imposing a disclosure requirement;
- a consideration of whether imposing a disclosure requirement interferes with the personal privacy at the person on whom it is served, or on the owner of the information, and the justification for that interference;
- a consideration of whether imposing a requirement interferes with the personal privacy at others who may be affected by it (collateral intrusion); and the justification for that interference;
- a consideration of why it is not reasonably practicable for the public authority to obtain the plain text of the protected material described in the application by some other method without serving a disclosure notice;
- an indication, where needed, of the urgency of the application with supporting justification.

Permission to serve a notice

4.7 Before a section 47 notice can be given in a particular case, a number of requirements must be met. These are set out in section 47 of the 2000 Act.

Although these tests are strictly imposed on the person proposing to give the notice, and not on the person granting permission for that notice to be given, they are clearly critical to any application for permission.

4.8 The requirements are that the person proposing to give a section 47 notice believes, on reasonable grounds, that:

- the person on whom the notice is to be served has possession of a key to the relevant protected information;
- imposing a disclosure requirement in respect of this information is necessary:
  - 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

- likely to be of value in carrying out the statutory powers or duties of the public authority making the application;

- what is sought to be achieved by imposing a disclosure requirement is proportionate; and

- it is not reasonably practicable for the public authority concerned to obtain the plain text of the relevant protected information without serving a disclosure notice.

4.9 The person deciding whether to grant permission will wish to scrutinise the application with these factors in mind, and considering also the privacy implications described in the application.

4.10 Information about the effect of serving a disclosure notice is set out in Section 7 of this code. Details of further statutory conditions which must be met if is proposed to demand disclosure at a key – rather than the plain text of protected information – are described in Section 8 of this code.

Retention of records

4.11 The relevant public authority must retain copies of all applications for permission to same a disclosure notice. Such applications, where appropriate, may be scrutinised by the relevant independent Commissioner with a statutory oversight role (see section 12 of this code). 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.

4.12 Where in urgent cases it has not been possible to make a written application for permission to give a section 47 notice, the relevant public authority should, as soon as possible after any such permission has been given, record in writing full details of the application as it was made.

[Duration of permissions - The code will cover. in detail, the duration of *permissions. In general terms, these will be tied to the duration* of *the underlying statutory power – e.g. interception as described in the code* of *practice for Part I of the 2000 Act]*

5 FORM OF NOTICES

5.1 This section describes the form that a section 47 notice should take.

Statutory requirements

5.2 The 2000 Act makes a number of stipulations about the form of a disclosure notice. By virtue of section 47(4) of the 2000 Act, all notices given by public authorities **must**:

a) be in writing[5];

b) describe the protected material to which the notice relates;

c) specify the grounds on which the notice is justified (e.g. as being necessary in the interests of national security);

d) contain details of the office, rank or position of the person actually serving the notice;

e) specify the office, rank or position of the person who has granted permission for the notice to be served (e.g. the Secretary of State) or the circumstances in which the person giving the notice permission became entitled to do so);

f) specify the time by which the notice is to be complied with; and

g) describe what disclosure is required (i.e. the plain text of protected information or a key) and how that requirement is to be fulfilled (to whom is the required information to be disclosed).

Notices requiring the disclosure of a key

5.3 Where a relevant public authority has obtained a direction that a key – rather than plain text – is required to be disclosed, the notice should make it clear, in accordance with section 48 of the 2000 Act, that the choice of which key to disclose (if there is more than one which can access the protected information or put it into an intelligible form), rests with the person on whom the notice is being served. For further information see Section 8 of this code (keys).

Secrecy requirement

5.4 Where permission has been granted for disclosure notice to include a secrecy provision (see section 9 of this code), the notice should make this clear and the recipient of the notice should be made aware of this provision.

5.5 Where a secrecy provision is imposed, the notice should also inform the recipient that he/she may by virtue of section 53(6) of the 2000 Act, approach a lawyer for advice about the effect of the notice.

[5] It is envisaged that, in time, disclosure notices should, where appropriate, the capable of being served electronically The 2000 Act allows for this. But there are detailed legal and practical considerations which need working through before this stage is reached.

5.6 The Act also permits certain disclosures to be made – where these are authorised by the person serving the notice or by the terms of the notice itself. For further information about this, see Section 6 of this code on Service on notices.

Penalties

5.7 Notices should inform the recipient of the penalties attached to the disclosure requirement:

- the offence of failure to comply with a notice (section 51 of the 2000 Act); and
- (where appropriate) the offence of "tipping off" (section 52 of the Act).

Authenticity of notices

5.8 It is essential that any pension served with a disclosure notice is able to confirm, where necessary, its authenticity. In addition to the statutory requirements detailed in paragraph 5.2 above, notices must always contain a specific identifier (a unique reference number) and the address of an office and public contact telephone number via which the recipient of a notice may, if he/she chooses, cheek its authenticity. A facility for providing an authenticity check should be available at whatever time the notice is being served. In addition, the person giving the disclosure notice should, at the time the notice is served, carry sufficient identification to confirm their office, rank or position and, if requested to do so, must produce that identification to the person being served with the notice.

It is not obvious how this would work in cases of extreme urgency where there is not time for the person on whom the notice is served to visit the office listed for authentication. In such a situation the use of a telephone number would not offer much assurance since it would be easy for any number listed to be manned by an accomplice of the person seeking to serve a false disclosure notice. At very least this telephone number would have to be a listed number that could be checked against a telephone directory.

Retention of records

5.9 There should be a central record held in each public authority of all disclosure notices authorised and served. These records should be retained for a period of at least 5 years from the time when the disclosure notice ceased to have affect. Where the records relate to a case which results in criminal or civil proceedings or appeal, they should be retained for a suitable period commensurate to any subsequent review.

Specimen notice

5.10 Specimen disclosure notices are set out at Appendix 1 and 2 of this code If, for exceptional reasons, it is not practicable to serve a notice in the format set out at Appendix 1 and 2, a written notice must still contain all the elements set out in paragraph 5.2 above.

6 SERVICE OF NOTICES

6.1 This section sets out the considerations involved in the service of section 47 notices by public authorities.

6.2 Disclosure notices may potentially be served on a wide variety of individuals, bodies or organisations. Individuals using encryption or businesses involved in producing or supplying encryption products or services, or using such technologies themselves could conceivably be in a position to disclose relevant information in an intelligible form (plain text) or a key required to put to such information into an intelligible form. In many cases, as a consequence of the way the technology works, it will be a person other than the individual whose protected information is of concern who will have access to a relevant key.

6.3 By virtue of section 47(2) of the 2000 Act, once an appropriate permission has been granted, a disclosure notice may be given to any person believed to have possession of a key to the relevant protected information. Section 54 provides that possession includes the right of immediate access, as well as possession by a subordinate. There may, therefore, be a number of people on whom a notice could be served.

6.4 It is important, in these circumstances, to consider carefully who should receive a notice. The starting position, subject to any operational considerations, should be to choose the person best able to comply.

6.5 But special considerations apply where a company or firm is involved. In order to respect ordinary principles of corporate responsibility and administration, sectors 47(5) and (6) of the Act require disclosure notices to be served on the most senior person within the organisation except in certain special circumstances (see the following paragraph). So before a notice is served on a company or firm the public authority concerned should seek to establish, so far as practicable, the identity of the appropriate senior person within the organisation concerned, and that person should receive the notice.

6.6 Section 47(7) of the Act provides that where special circumstances exist, notices need not be served on the senior person within an organisation. Such circumstances would include those where it is the senior person who is a target of the criminal investigation or is reasonably believed to be a criminal associate of the target.

Explaining the notice

6.7 The person giving the notice should, as far as practicable and necessary, take steps to explain to the recipient of the notice its contents and what is required to be done in pursuance of it. In particular, the person serving the notice should be prepared to explain:

- on what grounds the disclosure requirement is being imposed;
- 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 up to the recipient of the notice;
- any secrecy provision (if appropriate);
- the penalties attached to the notice;
- how the authenticity of the notice may be confirmed.

Secrecy requirement and authorised disclosures

6.8 In cases where a disclosure notice includes a secrecy requirement (see Section 9 of this code for further details), the person serving the notice (or the notice itself) may authorise certain disclosures without these constituting an offence of "tipping off".

6.9 This is particularly relevant where notices are served on a senior person within an organisation. That person may need assistance – technical or otherwise – from another within that organisation or another in order to comply with the terms of the notice. So the person serving the notice should, so far as is practicable, ascertain in advance, whom it is reasonable to permit a disclosure to be made to. If these details cannot be obtained in advance, the person serving the notice will need to take all reasonable steps, at the time the notice is given, to establish who else might reasonably need to be told about the notice in order that it may be complied with. These details should be noted on the relevant disclosure notice for the avoidance of doubt.

Copies of notices

6.10 A copy of the relevant disclosure notice must be given, for retention, to the person on whom the notice has been served. The public authority concerned must retain a copy of the notice for its own records.

Since in some cases the recipient is required to keep the existence of a disclosure notice secret, the issue of the protection that they are required to give to their written copies of such notices needs to be considered. While it unreasonable to expect private individuals to make provision for holding documents securely, they could, nevertheless, go to prison if this document were to be seen by someone else.

The expected standards to be applied by authorities for the safe physical storage of disclosure notices that involve secrecy requirements need to be specified. Where such notices are served on individuals or businesses that do not have secure document storage facilities of equivalent

or better standards, the authorities serving the notice must provide these to the recipients of such notices without charge.

7 EFFECT OF SERVING A NOTICE

7.1 This section describes the effect of serving a section 47 notice (a disclosure notice) requiring the disclosure of protected information in an intelligible form (plain text). Notices requiring the disclosure of keys themselves are dealt with in the following section.

7.2 The effect of serving a notice on a person who, at the time the notice is served, is in possession of both the protected information and a key to that information, is that:

- the person served with the notice can use any key of his/her choosing to put the information into an intelligible form (plain text) and disclose that in accordance with the details set out in the notice;

- or he/she can instead disclose a relevant key if he/she so chooses.

8 KEYS

8.1 This section concerns the circumstances when a direction may be imposed requiring that a key be handed over in response to a section 47 notice rather than the plaintext of protected information.

Authorisation

8.2 By virtue of section 49(1) of the 2000 Act, only the person granting permission for a disclosure notice to be given may give a direction that a key itself - rather than plain text - is required to be disclosed. Unless a disclosure notice contains such a specific statement, the person serving the notice may not demand that a key be disclosed. The details of permission levels are set out in Section 3 of this code.

Process for giving a direction that a key be disclosed*

8.3 The Act imposes extra tests for demanding keys, over and above those for requiring the disclosure of plain text. Keys may only be required to be disclosed when the extra statutory requirements set out in section 49(2) of the Act, described in the following paragraph, have been fulfilled.

8.4 The public authority seeking permission to serve a notice requiring the disclosure of a key will need to justify fully why a key itself is being sought, as well as setting out all the details as described in paragraph 4.5 of this code, in its application to the person who has authority to give permission for such a notice to be served. Specifically, the public authority will need to justify:

- why the circumstances of the particular case are "special" i.e. why the purposes for which a disclosure notice is being served would be defeated, in whole or in part, if a key itself was not required to be disclosed; and

- why it is believed that requiring the disclosure of a key is proportionate to what is sought to be achieved by imposing such a direction.

The word "special" is used in the legislation rather than "exceptional" as originally proposed. This has caused considerable uncertainty and concern about the precise circumstances in which keys could be seized and Ministers have indicated in response that further information on such circumstances would be provided in this Code of Practice. This has NOT been done since this and the following paragraphs lack the detail and the precision that is required to allay fears in respect of Government Access to Keys (GAK).

8.5 Circumstances will vary from case to case. But by way of illustration, consideration may be given to seeking permission to require the disclosure of a key where:

- trust is an issue - where there is doubt about the bone fides of the person or organisation being asked to comply with a disclosure requirement e.g. the person or organisation concerned is suspected of involvement in criminality;

- timeliness is an issue - if a person or organisation has the key to protected information but cannot, for whatever reason, carry out the necessary decryption and provide the relevant plain text quickly enough in time critical situations (and where the relevant authority can), requiring the disclosure of a key may be considered to be proportionate to what is sought to be achieved by imposing this demand;

*The concern about **trust** is better met without reference to keys by allowing a disclosure notice to impose a requirement on the recipient to prove that the offered plain text is genuine.*

*The concern about **timeliness** is not meaningful without a more detailed explanation of the sort of scenarios that are envisaged, the reaction times needed and the actions that law enforcement authorities might be expected to take as a result of any decryptions. It is very unlikely that UK law enforcement authorities could effectively counter threats of the character hinted at here without a very significant investment of taxpayer's money. In fact it seems most likely that the Ministry of Defence is the only government agency that could counter this sort of threat and they will have more effective approaches than any that might rely on GAK powers. This is simply not a credible requirement when expressed in such vague terms and cannot be a realistic justification for the powers being sought.*

8.6 It follows that these will not be issues where a public authority is dealing with a case involving persons or legitimate organisations not themselves of security concern or suspected of involvement in any criminality, and who can comply with a disclosure notice within the time required.

8.7 Before the person with appropriate authority to give permission for a disclosure notice to be served can direct that a key may be required, he/she must be satisfied that both statutory tests outlined in paragraph 8.4 above have been met.

If GAK powers remain in this legislation it will be imperative that the "special" circumstances are set out in detail in order to ensure that keys are seized only in exceptional circumstances, for example, where there is a direct and immediate threat to human life.

Choice of key

8.8 By virtue of section 48 of the Act, where a direction has been given to require that a key be disclosed, the recipient of the notice may choose which key or keys to disclose (if there is more than one which can carry out the required decryption).

Electronic signature keys

8.9 By virtue of section 47(9) of the Act, a disclosure notice shall not require the disclosure of any key which is intended to be used for the purpose only of generating electronic signatures and has not in fact been used for any other purpose.

8.10 But where there are reasonable grounds to believe that a key has been used for electronic signature and, additionally, confidentiality purposes, that key may be required to be disclosed under the terms of the 2000 Act.

**The Government has tabled an amendment, the effect of which would be to put a requirement, on the face of the legislation, that the mallets to be taken into account in deciding whether it is proportionate to require that a key be disclosed must include a consideration of the extent and nature of information (other than that to which the notice relates) which is protected by the relevant key.*

These provisions for ensuring the integrity of digital signatures will not protect the majority of signature keys that are currently in widespread use.

The keys used to provide digital signatures and those used for protecting information are most often controlled by passwords or pass-phrases. Such passwords will often be the same for both sorts of keys and even where this is not necessarily the case, the difficulty of remembering different passwords will often mean that key owners simply use identical ones.

It is hence quite likely that access to a password for an information protection key will also give access to the owner's signature key and this means that GAK powers will have a serious impact on the perceived integrity of digital signatures despite the effort made here to avoid this. In consequence GAK powers will reduce trust and confidence in Internet security provision and this, in turn, will have a serious impact on the UK's aspirations in e-commerce.

9 SECRECY REQUIREMENT AND "TIPPING OFF"

9.1 This section concerns the circumstances when a section 47 notice may contain a secrecy requirement.

9.2 Section 52 of the 2000 Act creates an offence where the recipient of a disclosure notice which explicitly contains a secrecy requirement, or a person who becomes aware of it, "tips off" or discloses to another that a notice has been served, or reveals its contents or the things done in pursuance of it. The provision is designed to preserve - but only where necessary - the coved nature of an investigation and to deter deliberate and intentional behaviour designed to frustrate statutory procedures and assist others to evade detection. There is a similar offence for unauthorised disclosures in Part I of the 2000 Act (section 18).

Restrictions

9.3 By virtue of section 52(2) of the 2000 Act, the person giving permission for the disclosure notice to be served must consent to a secrecy requirement being included in a disclosure notice. A secrecy requirement may not be imposed by the person serving the notice unless that consent has been obtained. The details of permission levels are set out in Section 3 of this code.

9.4 By virtue of section 52(3) of the 2000 Act, a secrecy requirement may only be imposed in certain cases. The first condition is that the protected information has come, or is likely to come, into the possession of the police, HM Customs and Excise or the security and intelligence agencies (Security Service, SIS, GCHQ). The second test is that it is reasonable, 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, to keep secret the means by which the information was obtained. It is enough, to meet this test, that there is a particular person from whom it is reasonable to withhold the information.

9.5 Disclosure notices served by public authorities other than those specifically named in the preceding paragraph may not include a secrecy requirement.

Imposing a secrecy requirement

9.6 The public authority proposing to include a secrecy requirement (which can only be the police, HM Customs and Excise or one of the security and intelligence agencies) must justify the proposed requirement. The person granting permission for the notice to be given must decide whether imposing a secrecy requirement is indeed justified.

9.7 For example, in a case involving an interception warrant personally authorised by the Secretary of State under Part I of the 2000 Act, it may be considered reasonable to include a secrecy requirement in a relevant disclosure notice in order to prevent the recipient of a notice being free to let the target of the relevant investigation know that his communications were being intercepted. This is because interception is necessarily secret, as the provisions of Part I of the 2000 Act confirm. But in a case where a computer containing protected material is seized during a search warranted under the Police and Criminal Evidence Act 1984, a secrecy requirement may not be justified since the search will have been overt.

9.8 As described in Sections 5 and 6 at this code, the fact that a disclosure notice contains a secrecy requirement should be made clear to the recipient of that notice.

*The "tipping-off" offence is meaningless in respect of a disclosure notice for keys since the Government has indicated that a seized key **can** be revoked – that is, a new key can be issued immediately to replace one that is seized provided that no reason is given for this action. Since keys are sometimes revoked for other reasons, all that is necessary to identify that a disclosure notice has been served is to revoke the key without comment while saying **in all other cases** "I revoke my key but not as a result of a disclosure notice".*

Statutory defences

9.9 Relevant authorities (i.e. those named in paragraph 9.4 above) should be aware that section 52 of the 2000 Act Contains statutory defences to the "tipping off" offence.

Automatic tipping-off

9.10 There is a feature of particular encryption software which, for security reasons, is specifically designed to give out an automatic warning when a key has been disclosed. The 2000 Act caters for this situation.

9.11 There is a specific defence in section 52(5) where the "tipping off" or disclosure occurred entirely as a result of software which is set up to give an automatic warning that a key has been disclosed and where, in addition, a person was not reasonably able to stop this from happening after being served with a disclosure notice.

Since key revocation is legal for seized keys, the key owner should be safe from prosecution provided that such software simply revokes keys without giving any reasons. But this paragraph seems to be suggesting that key revocation may not be legal for seized keys.

9.12 The person seeking permission to serve a disclosure notice should, so far as is practicable, establish whether the person to be served with the notice uses software that gives an automatic warning about key disclosure and if he/she does, whether it is reasonable, in all the circumstances, for the recipient of the notice to take steps to prevent this disclosure from happening.

As already indicated, if immediate key revocation is allowed for a seized key, the "tipping-off" offence becomes meaningless since it is trivial to circumvent. It makes no sense to threaten honest key owners with criminal prosecution for an offence that it is so easy to avoid. Maybe the legality of immediately revoking seized keys is not so straightforward as the Home Office would have us believe?

Legal advice

9.13 A person served with a disclosure notice which contains a secrecy requirement is, nevertheless, permitted to approach a professional legal adviser for advice about the effect of the notice.

9.14 Section 52(6) of the 2000 Act provides a statutory defence to ensure that persons may approach a legal professional for advice about the effect of the Part Ill provisions, and that advice may in turn be given, without either party being guilty of "tipping off". There is a further statutory defence in section 52(7) where a disclosure was made by a lawyer in connection with legal proceedings.

Authorised disclosure

9.17 It is not the intention of the Act to penalise individuals, within organisations for example, who have been served with a disclosure notice but need the assistance of another (perhaps an IT director) in complying with the terms of the notice.

9.18 So, as described in Sections 5 and 6 of this code the 2000 Act provides a statutory defence in section 52(9) against "tipping off" where a disclosure has been authorised by the terms of the disclosure notice or by the person serving it.

10 RECEIPT OF INFORMATION

10.1 This section concerns the practice for receiving the information required to be disclosed under a section 47 notice.

[This section and the next (Safeguards) will need to be developed in tandem with the ongoing project to establish the dedicated resource - the Technical Assistance Centre - which the Government has announced will be set up to assist public authorities over encrypted information]

10.2 As described in paragraph 5.2 of this code, disclose notices must describe the form and manner in which the required disclosure of information is to be made. Notwithstanding this, it is best practice that the person giving the notice seek, so far as possible, to agree with the person or organisation being served with the notice the manner in which the required disclosure is in practice to take place.

Keys disclosed in support of a statutory power to intercept communications

10.3 In circumstances in which a disclosure requirement for a key is necessary in support of a statutory power to intercept communications, then that key will be handled as SECRET[6] information from its handover to the person giving the notice or its transmission to any processing facility and during processing and storage within any processing facility. Once the handover has taken place, it shall be the duty of the

[6] Defined as: "The compromise of this information or material would be likely: to raise international tension; to damage seriously relations with friendly governments; to threaten life directly, or seriously prejudice public order or individual security or liberty; to cause serious damage to the operational effectiveness of security of UK or allied forces or the continuing effectiveness of highly valuable serurity or intelligence operations; to cause substantial material damage to national finances or economic and commercial interests"

person serving the notice or the official in charge of any processing facility to ensure physical or electronic transmission appropriate to SECRET material.

*The Government needs to make a clear statement indicating that it will protect all such information by **fully applying all appropriate and approved government standards for its protection**.*

10.4 Any person having access to a disclosed key shall be appropriately vetted. The person who has been given permission for the giving of a disclosure notice shall keep a record of all persons having access to each key and of the storage and destruction of each key.

*Vetting is just a small part of the personnel requirement. In particular all those who may be required to handle seized keys of any kind need to be trained in the procedures and approaches needed to handle cryptographic key material. Keys need to be specially marked as such and **special handling procedures beyond those used for SECRET material need to be employed**.*

Keys disclosed in support of all other lawful purposes

10.5 In the circumstances in which a disclosure requirement for a key is necessary in support of any power other than the exercise of any statutory power to intercept communications, then that key will be handled with the due care and attention required for evidential material. The person serving the notice may accord a higher level of security if this is necessary in the particular circumstances of the case.

10.6 Disclosure shall, so far as is practical in the circumstances of the case, be in the form most convenient to the person given notice. Once handover has taken place it shall be the duty of the person serving the notice to ensure physical or electronic transmission appropriate to the evidential status of the key and any material derived from its application to the protected information. It shall be the duty of the person serving the notice or the official in charge of any processing facility to protect the material from unauthorised disclosure.

The issues of key protection will be discussed later but it is incredible that all that is required here by this Code of Practice is 'due care and attention' at the discretion of the authorities involved. This is 'a million miles' from the care with which the Government treats its own critical cryptographic keys and secure information – it is beyond belief that anything less should be advocated.

11 SAFEGUARDS

11.1 This section concerns the arrangements for safeguarding information obtained under Part Ill of the 2000 Act. The statutory requirements are set out in section 53 to the Act.

[As stated on p.23 of this code, this section will need to be developed in tandem with the ongoing project to establish the new Technical Assistance Centre]

11.2 All keys *to* protected information obtained under a disclosure notice must be handled in accordance with approved safeguards. These may vary for different agencies and/or different classes of disclosure but must accord with the general principles set out in this code.

This Code of Practice must set out in detail all the procedures, standards and technical mechanisms required for the protection of seized keys for all authorities that might have any involvement in key seizure processes. It should be absolutely clear that such authorities would only be allowed to exercise powers for key seizure when they have a certificate of conformance to an agreed set of protection procedures and standards issued by an expert technical body reporting to an appropriate Commissioner.

11.3 The safeguards must enforce the statutory requirement to limit for each instance of disclosure of a key and the use which may be made of the key. The safeguards must set out provisions for disclosure, copying and destruction of any disclosed key.

Special Procedure Material

11.4 Upon application of a key to protected material, it may become apparent that the material thereby disclosed is subject to legal privilege, or is journalistic material or other special procedure material outside the scope of the lawful authority by which the protected information was acquired. In such circumstances all copies of the material thus disclosed shall be destroyed immediately. No use may be made of such material for any purpose. A record will be kept of all persons who have had access to such material and of the destruction of the material.

11.5 If discrete parts of the protected information itself can be identified as subject to privilege or special procedure material, that information should be deleted. However this may not take place if such an action carries the risk of damaging the remainder of the information or the evidential status of such information.

For this record to be meaningful it would need to describe in some form the information to which the record refers. It would not be enough to describe the protected information since this will not be sufficient to identify the information items that are outside the scope of the lawful authority. But once the nature of the unlawfully seen information is described it is then possible that the record itself will be unlawful.

Disclosure

11.6 The number of persons to whom any key, the detail of any key or the fact of possession of a key is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary to allow protected information to be made intelligible. This obligation applies equally to disclosure to additional persons within an agency, to disclosure outside the agency and to any data processing facility.

11.7 In the case of keys required to make intercept material intelligible, the obligation is enforced by prohibiting disclosure to persons who do not hold a required security clearance (see below), but also by the *need-to-know principle*. 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/she needs to know the information to carry out his/her duties. A record must be maintained of any disclosure.

The "need-to-know principle" is really designed for information in human readable form and is not really appropriate for cryptographic keys that are intended for machine use.

The critical issues for such keys are the details of all the technical environments in which they are stored and used and the way they are moved between such environments. Those in control of such keys will have to have complete confidence in the systems used to store, transmit and use them – they will need to be sure that they do not have any security properties that could result in the keys being copied, retained or transmitted to remote systems covertly. Moreover they will need to be certain that all the environments in which the keys exist are sufficiently secure to protect them from sophisticated external attacks mounted by highly expert teams with access to essentially unlimited computing resources.

At best the design and implementation of such computer systems poses an extreme technical challenge; at worst it will not be possible. This Code of Practice needs to set out all the details of such needs, how they will be met and the full costs involved.

11.8 In the case of keys required to make intelligible protected information other than intercept material, 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/she needs to know the information to process the protected information or to conduct a criminal prosecution.

Storage*

11.9 All keys disclosed under the 2000 Act should be stored in an appropriately secure manner. The person who gave the notice, or the official in charge of any processing facility, is responsible for ensuring that all keys are secured appropriately.

These are just words unless and until this Code of Practice sets out in full detail how this will be achieved.

**The Government has tabled an amendment to put, on the face of the Bill, a statutory requirement for keys to be stored in a secure manner.*

Copying

11.10 The number of copies made of any key or the detail of any key must be limited to the minimum that is necessary to allow protected information to be made intelligible. A record must be maintained of any copy made. Where protected information is put in an intelligible form using a disclosed key, and that intelligible information is used in criminal proceedings copies of the key will be required for evidential or disclosure purposes.

Destruction

11.11 Keys and all copies of keys must be destroyed as soon as they are no longer needed for any use under Section 53(2) of the Act. If any key is retained, its retention should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

These key seizure provisions are written around software based keys and no thought appears to have been given to keys held in hardware such as smart-cards, PCMCIA cards or high integrity anti-tamper devices. In addition, the issues involved in split keys are covered at length in the Bill but no thought is given here to the serious difficulties, costs and risks involved in reassembling such keys outside the environment in which this would normally be undertaken.

There are many different sorts of cryptographic keys in use and many different software and hardware environments in which they are designed to operate. Cryptographic keys and the immediately associated processing engines (e.g. smart-card processors) will generally be designed to protect the keys they hold by not allowing their use unless the environment in which access is requested meets stringent requirements. To use these keys within a GTAC environment will either require an enormous amount of highly specialised equipment or will have to be done in a way that puts the keys at risk.

None of the many critical issues involved in setting up and operating safe environments for the use of cryptographic keys have been properly described in this document.

Personnel Security

11.12 Any persons having access to a key which has been disclosed in support of a statutory power to intercept communications must be appropriately vetted. Such access is to be limited to as few individuals as is necessary to meet operational requirements.

Vetting is one of several requirements that will need to be met. Another is that all personnel will need to be fully trained in the handling of cryptographic key material.

11.13 In the circumstances in which a disclosure requirement for a key is necessary in relation to protected information other than intercept material, it shall be the duty of the person serving the notice to protect the material from unauthorised disclosure. While a key disclosed for such purposes will normally be unclassified, the person serving the notice may require that any key handed over shall be handled at a higher level of security if this is necessary in the particular circumstances of the case.

Abuse of Seized Keys or Derived Information

My thanks go to Yaman Akdeniz for this contribution. There is a major omission in this Code of Practice in that there is no coverage of any of the issues related to the misuse of seized keys or information (other than privileged information). When considering the precursor to the RIP Bill, the Trade and Industry Committee in its Fourteenth Report on the Draft Electronic Communications Bill, HC 862, 25 October, 1999 stated on paragraph 34 in relation to codes of practices related to Part III that:

> *"Provision has been made for the Secretary of State of Home Affairs to issue a code of practice 'in connection with the exercise or performance by persons (other than proposed Commissioner and Tribunal) of their powers and duties' under part III of the draft Bill. Such persons are to 'have regard for the code of practice' when performing their duties; but it is expressly provided that failure to comply with any provision of the code will NOT of itself lead to criminal or civil proceedings against the person concerned." Therefore the Committee stated that "the proposed code of practice may prove to be toothless" and "the impression is given by the legislation that infringements of the code of practice will go unpunished".*

The Government responded on 26 January, 2000, in the Third Special Report of the Trade and Industry Committee, HC199 that:

> *"The Government is considering carefully how the proposed statutory Code of Practice is to be best operated. The view of the Committee, ..., will be taken into account in bringing forward the RIP Bill".*

But we can now see that the draft Code of Practice contains no provisions of any kind covering the abuse of the powers provided in this legislation or the abuse of any keys or information obtained as a result of the use of such powers. Despite the Government commitment, no attempt has been made in this Code of Practice to highlight the potential problems of abuse, the way these should be tackled, the remedies that should be available or the need for disciplinary codes of conduct and offences to provide a basis for action when abuse is discovered. In short, as the T&I Committee predicted, the Code of Practice is toothless and gives the impression that any abuse of RIP powers will go unpunished.

OVERALL CONCLUSION

This Code of Practice does not specify how the interests of owners of seized keys will be safeguarded. At best it considers key protection only from a Government perspective and even here it sets very limited standards for the protection of keys that are not intercept related. Issues of abuse are not covered at all and the overall impression is left that there is no significant commitment to protect the interests of those who, through no fault of their own, are unfortunate enough to find themselves the targets of this legislation.

12 OVERSIGHT

12.1 This section deals with the independent oversight of the provisions in Part Ill of the 2000 Act.

Oversight

12.2 The Act provides for oversight, by independent Commissioners, of the permissions to same disclosure notices given by non-judicial figures and the adequacy of the arrangements for safeguarding information obtained under such notices.

12.3 As regards Part Ill of the Act, them are three independent Commissioners with relevant oversight responsibilities:

Interception of Communications Commissioner

12.4 So far as Part Ill of the 2000 Act is concerned, the Interception of Communications Commissioner, who is appointed by the Prime Minister, has a statutory duty to review:

- permissions given by the Secretary of State to same disclosure notices which relate to intercepted material or communications data; and

- the adequacy of the safeguards arrangements made by the Secretary of State for the protection of keys.

12.5 The Interception Commissioner is required to make an annual report to the Prime Minister, which is laid before Parliament and published.[7]

12.6 The Act gives the Interception Commissioner wide-ranging powers to require the production of documents and information. All persons involved in utilising the powers under Part Ill of the Act have a duty to comply with any request for information from or on behalf of the Interception Commissioner. If the Commissioner finds any contravention of the provisions of the Act (not already reported on by the Tribunal - see next section) or determines that any safeguards are inadequate, he or she will report this to the Prime Minister.

Intelligence Services Commissioner

12.7 So far as Part Ill of the Act is concerned, the Intelligence Services Commissioner, who is also appointed by the Prime Minister, has a statutory duty to review the following activities (so far as they do not fall to the Interception Commissioner to review):

- Secretary of State permissions for disclosure notices in respect of the security and intelligence agencies (Security Service, SIS, GCHQ);

- The use by the security and intelligence agencies and HM Forces (other than in Northern Ireland) of the powers in Part Ill of the Act;

- The adequacy of the safeguards arrangements for protecting keys by the security and intelligence agencies and HM Forces (other than as above).

[7] The Prime Minister may after consultation with the Commissioner exclude from the repaid to be laid before Parlhament any matter inclusion of which appears to him to be contrary to the public interest or which world otherwise be prejudicial to national security, the preventon or detection of serious crime, the economic well being of the UK or the continued discharge of the functions of any public authority whose actions are subject to review by the Commissionser.

12.8 As with the Interception Commissioner, the Intelligence Services Commissioner is required to make an annual report to the Prime Minister, which is laid before Parliament and published. The Act also gives the Intelligence Services Commissioner wide-ranging powers to require the production of documents and information as described in paragraph 12.6 above.

Chief Surveillance Commissioner

12.9 The 2000 Act adds to the remit of the Chief Surveillance Commissioner established under the Police Act 1997 the following functions as regards Part III of the Act (so far as these are not the responsibility of the Commissioners listed above):

- the exercise or performance of any person (other than a judicial authority) of the Part Ill powers; and

- the adequacy of the safeguards arrangements for protecting keys so far as these are not the responsibility of one of the other Commissioners.

This Commissioner needs expert technical staff to ensure that all authorities with RIP powers can properly protect the information and keys that they obtain through their use.

13 Complaints

13.1 This section deals with the independent complaints mechanism established in Part IV of the 2000 Act as it relates to the powers contained in Part Ill of the Act.

13.2 The 2000 Act establishes an independent Tribunal with powers to investigate and decide any case within its jurisdiction. It is made up of senior members of the legal profession and is independent of the Government.

13.3 The Tribunal has jurisdiction (among other things) to hear complaints about the actions of the intelligence services or anyone acting on their behalf; disclosure notices given with the permission of the Secretary of State and any disclosure or use of keys to protected information.

Information leaflet

13.4 Public authorities who Utilise the powers contained in Part Ill of the 2000 Act should ensure that the information leaflet “Complaints about the exercise of powers under the Regulation of Investigatory Powers Act 2000” is readily available at any public office of the authority concerned.

Appendix 1

SECRECY REQUIREMENT: PLEASE READ PARAGRAPH 10 IMMEDIATELY*

REGULATION OF INVESTIGATORY POWERS ACT 2000

Section 47 notice

This notice imposes a legal obligation on you. Failure to comply is an offence and may result in prosecution. If you are in any doubt about the effect of this notice, or how to comply with it, you should consult a professional legal adviser.

To: *[named recipient of notice]*

Disclosure requirement

1. Pursuant to section 47(2) of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"), I hereby require you to disclose the information described below in an intelligible form.

2. The information to which this notice relates is:

[description of protected information]

Reason for notice

3. 1 believe that this notice is necessary in the interests of *national* security/for the purpose of preventing or detecting crime i the interests of the economic well-being of the United Kingdom;*

or

I believe that this notice is likely to be of value for purposes connected with the exercise or performance by *[name of public authority]* of *[specify statutory power or duty]**

Permission for notice

4. By law, this notice may only be given by a person who has the appropriate permission to give it. I have been granted permission to give this notice by *[specify office, rank or position of person giving permission to same the notice]. [Or, I am entitled to give this notice because...]*

Compliance

If you are able to disclose the information in intelligible form

5. You must disclose the information described in paragraph 2 of this notice no later than *[time]*

to:

[details of appropriate officer].

6. Alternatively, you may if you choose disclose any key which to the information to the same officer and within the same period.

If you are not able to disclose the information in intelligible form

7. If you are not in possession of the information described in paragraph 2 of this notice, you must disclose any key to the information that is in your possession.

8. If you are in possession of the information, but the keys in your possession do not enable you to put it into intelligible form, you must nevertheless disclose any keys in your possession which facilitate that process.

Choice of key

9. Where you choose to disclose a key, or where this notice requires you to do so, you may select which key to disclose. If you are able to disclose a key or combination of keys which will put the information into intelligible form, no further disclosure is required of you. And if there are several keys or combinations of keys whose disclosure would discharge your obligation, the choice of which to disclose is yours.

Secrecy requirement*

10. By virtue of section 52 of the 2000 Act, I hereby require you to keep secret the giving of this notice, its contents and the things done in pursuance of it. **Disclosure, except as described below, is an offence and may result in prosecution.**

11. This does not affect your right to consult a professional legal adviser for advice about the effect of this notice.

12. By virtue of section 52(9) of the 2000 Act, I also authorise you to disclose to the persons described below the fact that this notice has been given:

[details of persons to whom a disclosure is authorised]

13. If you wish to discuss this notice with any other person, you should consult me first. You must not make any other disclosures without my authority.

Validity

14. This notice is not valid unless signed and dated below by the person who has been given the appropriate permission to give it. If necessary, the authenticity of this notice may be confirmed by contacting the following telephone number and quoting the unique identification number given at the foot of this notice

[telephone contact point to confirm *authenticity]*

[office, rank or *position of* person serving t*he notice]* *[date]*

[unique notice identifier – xxx/2000]

Delete as appropriate

Penalties

By virtue of section 51(1) of the 2000 Act, *a* person to whom a section 47 notice has been given is guilty of an offence if he fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice. A person guilty of such an offence is liable-

- On conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

- On summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

By virtue of section 52(4) of the 2000 Act, a person who makes a disclosure to any other person of anything that he is required by a section 47 notice to keep secret shall be guilty of an offence and liable-

- On conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both;

- On summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

Appendix 2

SECRECY REQUIREMENT: PLEASE READ PARAGRAPH 7 IMMEDIATELY*

REGULATION OF INVESTIGATORY POWERS ACT 2000

Section 47 notice requiring disclosure of key

This notice imposes a legal obligation on you. Failure to comply is an offence and may result in prosecution. If you are in any doubt about the effect of this notice, or how to comply with it, you should consult a professional legal adviser.

To: *[named recipient of notice]*

Disclosure requirement

1. Pursuant to section 47(2) of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"), I hereby require you to disclose a key to the *information* described below.

2. The information to which this notice relates is.

[descripion of protected information]

Reason for notice

3. I believe that this notice is necessary 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

I believe that this notice is likely to be of value for purposes connected with the exercise or performance by *[name of public authority]* of *[specify statutory power or duty]*.*

Permission for notice

4, By law, this notice may only be given by a person who has the appropriate permission to give it. I have been granted permission to give this notice by *[specify office, rank or position of person giving permission to serve the notice]*. *[Or, I am entitled to give this notice because…]*

Compliance

5. This notice can only be complied with by disclosing a key to the information described in paragraph 2. You must disclose the key *[describe form and manner of disclosure]* no later than [*time].*

to:

[details of appropriate officer].

Choice of key

6. If you are able to disclose a key or combination of keys which will put the information into intelligible form, no further disclosure is required of you. And if there are several keys or combinations of keys whose disclosure would discharge your obligation, the choice of which to disclose is yours.

Secrecy requirement*

7. By virtue of section 52 of the 2000 Act, I hereby require you to keep secret the giving of this notice, its contents and the things done in pursuance of it. **Disclosure, except as described below, is an offence and may result in prosecution.**

ADD: You are, however, allowed to revoke this key immediately, and to issue a new key, provided that you do not reveal to others the reasons for your action.

8. This does not affect your right to consult a professional legal adviser for advice about the effect of this notice.

9. By virtue of section 52(9) of the 2000 Act, I also authorise you to disclose to the persons described below the fact that this notice has been given:

[details of persons to whom a disclosure is authorised]

10. If you wish to discuss this notice with any other person, you should consult me first. You must not make any other disclosures without my authority.

Validity

11. This notice is not valid unless signed and dated below by the person who has been given the appropriate permission to give it. If necessary, the authenticity of this notice may be confirmed by contacting the following telephone number and quoting the unique identification number given at the foot of this notice

[telephone contact point to confirm authenticity]

[offlice, rank or position of person serving the notice] *[date]*

[unique notice identifier- xxxx/2000]

'Delete as appropriate

Penalties

By virtue of section 51(1) of the 2000 Act, a person to whom a section 47 notice has been given is guilty of an offence if he fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice. A person guilty of such an offence is liable-

- On conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

- On summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

By virtue of section 52(4) of the 2000 Act, a person who makes a disclosure to any other person of anything that he is required by a section 47 notice to keep secret shall be guilty of an offence and liable-

- On conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both;

- On summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.