Interception of Communications

Code of Practice

Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003

Interception of Communications

Code of Practice

(Made pursuant to Section 61 of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003.

CONTENTS

Section 1: GENERAL

Section 2: GENERAL RULES ON INTERCEPTION WITH A WARRANT

Section 3: SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Section 4: INTERCEPTION WARRANTS (SECTION 7(1))

Section 5: INTERCEPTION WARRANTS (SECTION 7(4))

Section 6: SAFEGUARDS

Section 7: DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

Section 8: INDEPENDENT SCRUTINY

Section 9: COMPLAINTS

Section 10: INTERCEPTION WITHOUT A WARRANT

1. GENERAL

1.1 This Code of Practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003 ("the Law"). It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. It is primarily intended for use by those public authorities listed in section 6(1) of the Law. It will also prove useful to postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.

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

2. GENERAL RULES ON INTERCEPTION WITH A WARRANT

2.1 There are a limited number of persons by whom, or on behalf of whom, applications for interception warrants may be made. These persons are:

- The Chief Officer of the Island Police;
- The Chief Officer of the Customs and Excise Department;
- The Intelligence Services;

- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the Bailiwick.

2.2 All interception warrants are issued by one of the Law Officers; in this Code references to Her Majesty's Procureur include Her Majesty's Comptroller. Before issuing an interception warrant, Her Majesty's Procureur must believe that what the action seeks to achieve is necessary for one of the following section 5(3) purposes:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the Bailiwick;

and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

Necessity and Proportionality

2.4 Obtaining a warrant under the Law will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. The Law recognises this by first requiring that Her Majesty's Procureur believes that the authorisation is necessary on one or more of the statutory grounds set out in section 5(3) of the Law. This requires him to believe that it is necessary to undertake the interception which is to be authorised for a particular purpose falling within the relevant statutory ground.

2.5 Then, if the interception is necessary, Her Majesty's Procureur must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means. Further, all interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Implementation of Warrants

2.6 After a warrant has been issued it will be forwarded to the person to whom it is addressed, which in practice will be the person or agency that submitted the application. The Law (section 10) then permits the intercepting agency to carry out the interception, or to require the assistance of other persons in giving effect to the warrant. Warrants cannot be served on those outside the jurisdiction of the Bailiwick.

Provision of Reasonable Assistance

2.7 Any postal or telecommunications operator (referred to as communications service providers) in the Bailiwick may be required to provide assistance in giving effect to an interception. The Law places a requirement on postal and telecommunications operators to take all such steps for giving effect to the warrant as are notified to them (section 10(4) of the Law). But the steps that may be required are limited to those which it is reasonably practicable to take (section 10(5)). If there is disagreement about what is reasonably practicable, it will be for Her Majesty's Procureur to decide whether to press forward with civil proceedings or whether to institute criminal proceedings.

2.8 Where the intercepting agency requires the assistance of a communications service provider in order to implement a warrant, they should provide the following to the communications service provider:

- A copy of the warrant instrument signed and dated by Her Majesty's Procureur;

- The relevant schedule for that service provider setting out the numbers, addresses or other factors identifying the communications to be intercepted;

- A covering document from the intercepting agency requiring the assistance of the communications service provider and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all postal and telecommunications operators who maintain an intercept capability.

Provision of Intercept Capability

2.9 Whilst all persons who provide a postal or telecommunications service are obliged to provide assistance in giving effect to an interception, persons who provide a public postal or telecommunications service, or plan to do so, may also be required to provide a reasonable intercept capability. The obligations that Her Majesty's Procureur considers reasonable to impose on such persons to ensure they have such a capability will be set out in regulations made by the Home Affairs Committee following wider consultation, and approved by the States of Deliberation. Her Majesty's Procureur may then serve a notice upon a communications service provider setting out the steps they must take to ensure they can meet these obligations. A notice will not be served without consultation over the content of the notice between the law enforcement agencies and the service provider having previously taken place. When served with such a notice, a communications service provider, if he feels it unreasonable, will be able to refer that notice to the Technical Advisory Panel on the reasonableness of the technical requirements and capabilities that are

being sought. Details of how to submit a notice to the Panel will be provided either before or at the time the notice is served.

2.10 Any communications service provider obliged to maintain a reasonable intercept capability will be provided with a handbook which will contain the basic information they require to respond to requests for reasonable assistance for the interception of communications.

Duration of Interception Warrants

2.11 All interception warrants are valid for an initial period of three months. Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/ economic well-being grounds are valid for a further period of six months.

2.12 Where a change in circumstance prior to the set expiry date leads the intercepting agency to consider it no longer necessary or practicable for the warrant to be in force, it should be cancelled with immediate effect.

Stored Communications

2.13 Section 2(7) of the Law defines a communication in the course of its transmission as also encompassing any time when the communication is being stored on the communication system in such a way as to enable the intended recipient to have access to it. This means that a warrant can be used to obtain both communications that are in the process of transmission and those that are being stored on the transmission system.

2.14 Stored communications may also be accessed by means other than a warrant. If a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (eg. under the Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law, 2003) or a search warrant.

3. SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral Intrusion

3.1 Consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved. An application for an interception warrant should draw attention to any circumstances which give rise to an unusual degree of collateral infringement of privacy, and this will be taken into account by Her Majesty's Procureur when considering a warrant application. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as directly relevant to the operation, consideration should be given to applying for separate warrants covering those individuals.

Confidential Information

3.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material (see paragraphs 3.9-3.11). For example, extra consideration should be given where interception might involve communications between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

Communications Subject to Legal Privilege

3.3 Section 24 of the Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law 2003 describes those matters that are subject to legal privilege. Legal privilege does not apply to communications made with the intention of

furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the lawyer is intending to hold or use the information for a criminal purpose. But privilege is not lost if a lawyer is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 The Law does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications is particularly sensitive and is therefore subject to additional safeguards under this Code. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to some other material which has been sought.

3.6 In general, any application for a warrant which is likely to result in the interception of legally privileged communications should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. This assessment will be taken into account by Her Majesty's Procureur in deciding whether an interception is necessary under section 5(3) of the Law and whether it is proportionate. In such circumstances, Her Majesty's Procureur will be able to impose additional conditions such as regular reporting arrangements so as to be able to exercise his discretion on whether a warrant should continue to be authorised. In those cases where communications which include legally privileged communications have been intercepted and retained, the matter should be reported to the Commissioner during his inspections and the material be made available to him if requested.

3.7 Where an Advocate or other professional legal adviser is the subject of an interception, it is possible that a substantial proportion of the communications

which will be intercepted will be between the lawyer and his client(s) and will be subject to legal privilege. Any case where a lawyer is the subject of an investigation should be notified to the Commissioner during his inspections and any material which has been retained should be made available to him if requested.

3.8 In addition to the safeguards governing the handling and retention of intercept material as provided for in section 12 of the Law, persons who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege. Where there is doubt as to whether the communications are subject to legal privilege, advice should be sought from the Law Officers. Similar advice should also be sought where there is doubt over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.9 Similar consideration to that given to legally privileged communications must also be given to the interception of communications that involve confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

3.10 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his official capacity, and where the individual

being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their particular faith.

3.11 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4. INTERCEPTION WARRANTS (SECTION 7(1))

4.1 This section applies to the interception of communications by means of a warrant complying with section 7(1) of the Law. This type of warrant may be issued in respect of the interception of communications carried on any postal service or telecommunications system as defined in section 2(1) of the Law (including a private telecommunications system). Responsibility for the issuing of interception warrants rests with the Law Officers.

Application for a Section 7(1) Warrant

4.2 An application for a warrant is made to Her Majesty's Procureur. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.

- Person or premises to which the application relates (and how the person or premises feature in the operation).

- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.

- Description of the conduct to be authorised as considered necessary in order to carry out the interception, where appropriate.

- An explanation of why the interception is considered to be necessary under the provisions of section 5(3).

- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

- A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.

- Where an application is urgent, supporting justification should be provided.

- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 12 of the Law.

Authorisation of a Section 7(1) Warrant

4.3 Before issuing a warrant under section 7(1), Her Majesty's Procureur must believe the warrant is necessary

- in the interests of national security;

- for the purpose of preventing or detecting serious crime; or

- for the purpose of safeguarding the economic well-being of the Bailiwick.

4.4 In exercising his power to issue an interception warrant for the purpose of safeguarding the economic well-being of the Bailiwick (as provided for by section 5(3)(c) of the Law), Her Majesty's Procureur will consider whether the economic well-being of the Bailiwick which is to be safeguarded is, on the facts of each case, directly related to national security. Her Majesty's Procureur will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the Bailiwick and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the Bailiwick which is to be safeguarded is directly related to national security on the facts of the case.

4.5 Her Majesty's Procureur must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, Her Majesty's Procureur must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

Format of a Section 7(1) Warrant

4.6 Each warrant comprises two sections, a warrant instrument signed by Her Majesty's Procureur listing the subject of the interception or the set of premises, a copy of which each communications service provider will receive, and a schedule or set of schedules listing the communications to be intercepted. Only the schedule relevant to the communications that can be intercepted by the specified communications service provider will be provided to that service provider.

4.7 The warrant instrument should include:

- The name or description of the interception subject or of a set of premises in relation to which the interception is to take place;

- A warrant reference number.

4.8 The scheduled part of the warrant will comprise one or more schedules. Each schedule should contain:

- The name of the communication service provider, or the other person who is to take action;

- A warrant reference number;

- A means of identifying the communications to be intercepted.

Modification of Section 7(1) warrant

4.9 Interception warrants may be modified under the provisions of section 9 of the Law. A warrant may only be modified by one of the Law Officers.

4.10 A modification to the warrant may include the addition of a new schedule relating to a communication service provider on whom a copy of the warrant has not been previously served. Modifications made in this way expire at the same time as the warrant expires. There also exists a duty to modify a warrant by deleting a communication identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identifier, the relevant communications service provider must be advised and interception suspended before the modification instrument is signed.

Renewal of a Section 7(1) Warrant

4.11 Her Majesty's Procureur may renew a warrant at any point before its expiry date. Applications for renewals must be made to Her Majesty's Procureur and

should contain an update of the matters outlined in paragraph 4.2 above. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of the purposes in section 5(3).

4.12 Where Her Majesty's Procureur is satisfied that the interception continues to meet the requirements of the Law he may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/ economic well-being grounds, the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

4.13 A copy of the warrant renewal instrument will be forwarded by the intercepting agency to all relevant communications service providers on whom a copy of the original warrant instrument and a schedule have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the person or premises described in the warrant.

Warrant Cancellation

4.14 Her Majesty's Procureur is under a duty to cancel an interception warrant if, at any time before its expiry date, he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of the Law. Intercepting agencies will therefore need to keep their warrants under continuous review.

4.15 The cancellation instrument should be addressed to the person to whom the warrant was issued (the intercepting agency) and should include the reference number of the warrant and the description of the person or premises specified in the warrant. A copy of the cancellation instrument should be sent to those communications service providers who have held a copy of the warrant instrument and accompanying schedule during the preceding twelve months.

Records

4.16 The independent scrutiny regime allows the Commissioner appointed under the Law to inspect the warrant application upon which Her Majesty's Procureur based his decision, and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he may require:

- all applications made for warrants complying with section 7(1) and applications made for the renewal of such warrants.

- all warrants, and renewals and copies of schedule modifications (if any).

- where any application is refused, the grounds for refusal as given by the Her Majesty's Procureur.

- the dates on which interception is started and stopped.

4.17 Records shall also be kept of the arrangements by which the requirements of section 12(2) (minimisation of copying and destruction of intercepted material) and section 12(3) (destruction of intercepted material) are to be met. For further details see section on "Safeguards".

4.18 The term "intercepted material" is used throughout to embrace copies, extracts or summaries made from the intercepted material as well as the intercept material itself.

5. INTERCEPTION WARRANTS (SECTION 7(4))

5.1 This section of the Code applies to the interception of external communications by means of a warrant complying with section 7(4) of the Law. External communications are defined by the Law to be those which are

sent or received outside the British Islands. (British Islands means the United Kingdom, the Channel Islands and the Isle of Man). Such communications include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. Responsibility for the issuing of such interception warrants rests with Her Majesty's Procureur.

Application for a Section 7(4) Warrant

5.2 An application for a warrant is made to Her Majesty's Procureur. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.

- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the operation where this is relevant.

- Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate.

- The certificate that will regulate examination of intercepted material.

- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes.

- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

- A consideration of any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.

- Where an application is urgent, supporting justification should be provided.

- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 13(2)-13(6) of the Law.

- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 12 and 13 of the Law.

Authorisation of a Section 7(4) warrant

5.3 Before issuing a warrant under section 7(4), Her Majesty's Procureur must believe that the warrant is necessary:

- in the interests of national security;

- for the purpose of preventing or detecting serious crime; or

- for the purpose of safeguarding the economic well-being of the Bailiwick;

5.4 In exercising his power to issue an interception warrant for the purpose of safeguarding the economic well-being of the Bailiwick (as provided for by section 5(3)(c) of the Law), Her Majesty's Procureur will consider whether the economic well-being of the Bailiwick which is to be safeguarded is, on the

facts of each case, directly related to national security. Her Majesty's Procureur will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the Bailiwick and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the Bailiwick which is to be safeguarded is directly related to national security on the facts of the case.

5.5 Her Majesty's Procureur must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, Her Majesty's Procureur must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

5.6 When Her Majesty's Procureur issues a warrant of this kind, it must be accompanied by a certificate in which Her Majesty's Procureur certifies that he considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. Her Majesty's Procureur has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 13(2) to section 13(6) is, in fact, read, looked at or listened to. The Commissioner is under a duty to review the adequacy of those arrangements.

Format of a Section 7(4) Warrant

5.7 Each warrant is addressed to the person who submitted the application. This person may then serve a copy upon such providers of communications services as he believes will be able to assist in implementing the interception. Communications service providers will not receive a copy of the certificate.

The warrant should include the following:

- A description of the communications to be intercepted

- The warrant reference number

Modification of a section 7(4) warrant

5.8 Interception warrants may be modified under the provisions of section 9 of the Law. The warrant may only be modified by Her Majesty's Procureur. In these cases a statement of that fact must be endorsed on the modifying instrument. Any modification will expire at the same time as the rest of the warrant.

Renewal of a Section 7(4) Warrant

5.9 Her Majesty's Procureur may renew a warrant at any point before its expiry date. Applications for renewals are made to Her Majesty's Procureur and contain an update of the matters outlined in paragraph 5.2 above. In particular, the applicant must give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of purposes in section 5(3).

5.10 Where Her Majesty's Procureur is satisfied that the interception continues to meet the requirements of the Law he may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/ economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

5.11 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument will be forwarded by the intercepting agency to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the communications to be intercepted.

Warrant Cancellation

5.12 Her Majesty's Procureur will cancel an interception warrant if, at any time before its expiry date, he is satisfied that the warrant is no longer necessary on grounds falling within Section 5(3) of the Law.

5.13 The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those communications service providers, if any, who have given effect to the warrant during the preceding twelve months.

Records

5.14 The independent scrutiny regime allows the Commissioner to inspect the warrant application upon which Her Majesty's Procureur based his decision, and the applicant may be required to justify the content. Each intercepting agency should keep, so to be made available for scrutiny by the Commissioner, the following:

- all applications made for warrants complying with section 7(4), and applications made for the renewal of such warrants.

- all warrants and certificates, and copies of renewal and modification instruments (if any).

- where any application is refused, the grounds for refusal as given by the Her Majesty's Procureur.

- the dates on which interception is started and stopped.

Records shall also be kept of the arrangements in force for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 13(2) – 13(6) of the

Law in accordance with section 12 of the Law. Records shall be kept of the arrangements by which the requirements of section 12(2) (minimisation of copying and distribution of intercepted material) and section 12(3) (destruction of intercepted material) are to be met. For further details see the section below on "Safeguards".

6. SAFEGUARDS

6.1 All material (including related communications data) intercepted under the authority of a warrant complying with section 7(1) or section 7(4) of the Law must be handled in accordance with safeguards which Her Majesty's Procureur has approved in conformity with the duty imposed upon him by the Law. These safeguards are made available to the Commissioner, and they must meet the requirements of section 12 of the Law which are set out below. In addition, the safeguards in section 13 of the Law apply to warrants complying with section 7(4). Any breach of these safeguards must be reported to the Commissioner.

6.2 Section 12 of the Law requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorised purposes. The authorised purposes defined in section 12(4) of the Law include:

- if the material continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the Bailiwick;

- if the material is necessary for facilitating the carrying out of the functions of Her Majesty's Procureur under Chapter I of Part I of the Law;

- if the material is necessary for facilitating the carrying out of any functions of the Commissioner or the Tribunal;

- if the material is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution.

6.3 Section 13 provides for additional safeguards in relation to material gathered under section 7(4) warrants, requiring that the safeguards:

- ensure that intercepted material is read, looked at or listened to by any person only to the extent that the material is certified;

- regulate the use of selection factors that refer to individuals known to be for the time being in the British Islands.

Her Majesty's Procureur must ensure that the safeguards are in force before any interception under warrants complying with section 7(4) can begin. The Commissioner is under a duty to review the adequacy of the safeguards.

Dissemination of Intercepted Material

6.4 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 12(4) of the Law. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the

recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

6.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

Copying

6.6 Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 12(4) of the Law. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

6.7 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers. The details of what such a requirement will mean in practice for communications service providers will be set out in the discussions they will be having with the law enforcement agencies before a Section 11 Notice is served (see paragraph 2.9).

Destruction

6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 12(3) of the Law.

Personnel security

6.9 Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

7. DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

7.1 Section 12(3) of the Law states the general rule that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorised under the Law. Section 12(4) specifies the authorised purposes for which retention is necessary.

7.2 This part of the Code applies to the handling of intercepted material in the context of criminal proceedings where the material has been retained for one of the purposes authorised in section 12(4) of the Law. For those law enforcement agencies who would ordinarily have responsibilities to provide disclosure in criminal proceedings, this includes those rare situations where destruction of intercepted material has not taken place in accordance with section 12(3) and where that material is still in existence after the commencement of a criminal prosecution, retention having been considered

necessary to ensure that a person conducting a criminal prosecution has the information he needs to discharge his duty of ensuring its fairness (section 12(4)(d)).

Exclusion of Matters from Legal Proceedings

7.3 The general rule is that neither the possibility of interception nor intercepted material itself plays any part in legal proceedings. This rule is set out in section 14 of the Law, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Law (or under the Interception of Communications (Bailiwick of Guernsey) Law, 1997). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves "equality of arms" which is a requirement under Article 6 of the European Convention on Human Rights.

7.4 Section 15 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exceptions in subsections (6) to (11).

Disclosure to a Prosecutor

7.5 Section 15(6)(a) provides that intercepted material obtained by means of a warrant and which continues to be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

7.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of him by his duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he is given access under section 15(6)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.

7.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The

normal expectation is, still, for the intercepted material to be destroyed in accordance with the general safeguards provided by section 12. The exceptions only come into play if such material has, in fact, been retained for an authorised purpose. Because the authorised purpose given in section 5(3)(b) ("for the purpose of preventing or detecting serious crime") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the section 12(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.

7.8 Whatever the circumstances, section 15(6)(a) recognises the duty on prosecutors, acknowledged by customary law, to review all available material to make sure that the prosecution is not proceeding unfairly. 'Available material' will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorised purpose.

7.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of the holder of this material the prosecutor should be informed that a warrant has been issued under section 5 and that material of possible relevance to the case has been intercepted.

7.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, he will decide how the prosecution, if it proceeds, should be presented.

Disclosure to a Judge

7.11 Section 15(6)(b) recognises that there may be cases where the prosecutor, having seen intercepted material under subsection (7)(a), will need to consult the trial judge, who will in most cases be the Bailiff. Accordingly, it provides for the Bailiff to be given access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.

7.12 This access will be achieved by the prosecutor inviting the Bailiff to make an order for disclosure to him alone, under this subsection. This is an exceptional procedure; normally, the prosecutor's functions under subsection (6)(a) will not fall to be reviewed by the Bailiff. To comply with section 14(1), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.

7.13 The Bailiff may, having considered the intercepted material disclosed to him, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of section 14(1), it must not reveal the fact of interception. This is likely to be a very unusual step. The Law only allows it where the Bailiff considers it essential in the interests of justice.

7.14 Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

8. INDEPENDANT SCRUTINY

8.1 The Law provides for a Commissioner whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of the Law.

8.2 This Code does not cover the exercise of the Commissioner's functions. However, it will be the duty of any person who uses the above powers to comply with any request made by the Commissioner to provide any information as he requires for the purpose of enabling him to discharge his functions.

9. COMPLAINTS

9.1 The Law establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the States of Deliberation or any Committee or public administrative body in the Bailiwick. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

9.2 This Code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

The Secretary to the Tribunal,
Investigatory Powers Tribunal
PO Box 82,
Guernsey GY1 4BR.

10. INTERCEPTION WITHOUT A WARRANT

10.1 Section 1(5) of the Law permits interception without a warrant in the following circumstances:

- where it is authorised by or under sections 3 or 4 of the Law (see below);

- where it is in exercise, in relation to any stored communication, of some other statutory power exercised for the purpose of obtaining information or of taking possession of any document or other property, for example, the obtaining of a production order under Schedule 1 to the Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law, 2003 (PPACE) for stored data to be produced.

Interception in accordance with a warrant under section 5 of the Law is dealt with under parts 2, 3, 4 and 5 of this Code.

10.2 For lawful interception which takes place without a warrant, pursuant to sections 3 or 4 of the Law or pursuant to some other statutory power, there is no prohibition in the Law on the evidential use of any material that is obtained as a result. The matter may still, however, be regulated by the exclusionary rules of evidence to be found in the common law, in section 78 of PPACE, and/or pursuant to the Human Rights (Bailiwick of Guernsey) Law, 2000.

Interception with the Consent of both Parties

10.3 Section 3(1) of the Law authorises the interception of a communication if both the person sending the communication and the intended recipient(s) have consented to its interception, or where the person conducting the interception has reasonable grounds for believing that all parties have consented to the interception.

Interception with the consent of one party

10.4 Section 3(2) of the Law authorises the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorised under Part II of the Law. Further details can be found in Chapter 4 of the Covert Surveillance Code of Practice and in Chapter 2 of the Covert Human Intelligence Sources Code of Practice.

Interception for the purposes of a Communication Service Provider

10.5 Section 3(3) of the Law permits a communication service provider or a person acting upon their behalf to carry out interception for purposes connected with the operation of that service or for purposes connected with the enforcement of any enactment relating to the use of the communication service.

Lawful Business Practice

10.6 Section 4(2) of the Law enables the Home Affairs Committee to make Regulations setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. These regulations apply equally to public authorities (*see the Regulation of Investigatory Powers (Lawful Business Practice) Regulations, 2004*).