TURKS AND CAICOS ISLANDS

INTERCEPTION OF COMMUNICATIONS ORDINANCE 2022

(Ordinance 23 of 2022)

ARRANGEMENT OF SECTIONS

Chapter 2

EQUIPMENT INTERFERENCE

Chapter 3

MODIFICATION AND CANCELLATION OF WARRANTS AND REPORT

Chapter 4

IMPLEMENTATION OF WARRANTS

Chapter 5

CONFIDENTIALITY AND SAFEGUARDS

PART IV

PROTECTED INFORMATION

PART V

COMMUNICATIONS DATA

PART VI

INTERCEPTION EQUIPMENT

PART VII

MISCELLANEOUS

INTERCEPTION OF COMMUNICATIONS ORDINANCE 2022

(Ordinance 23 of 2022)

Assent……27th October 2022

Publication in Gazette……28th October 2022

Commencement…… in accordance with section 1

AN ORDINANCE TO MAKE PROVISION FOR THE LAWFUL INTERCEPTION OF COMMUNICATIONS, EQUIPMENT INTERFERENCE AND THE ACQUISITION OF COMMUNICATIONS DATA; THE TREATMENT OF MATERIAL HELD AS A RESULT OF SUCH INTERCEPTION, EQUIPMENT INTERFERENCE OR ACQUISITION; AND FOR CONNECTED PURPOSES.

ENACTED by the Legislature of the Turks and Caicos Islands.

PART I

PRELIMINARY

Short title and commencement

1. This Ordinance may be cited as the Interception of Communications Ordinance 2022 and shall come into force on such day as the Governor may appoint by Notice published in the *Gazette*.

Interpretation

2. (1) In this Ordinance—

"attorney-at-law" has the same meaning given to it in the Legal Profession Ordinance;

"authorised officer" means—

(a) the Commissioner of Police;

(b) the Deputy Commissioner of Police;

(c) a person for the time being lawfully exercising the functions of a person mentioned in paragraph *(a) or (b)*;

"Commissioner of Police" means the Commissioner of Police appointed under section 91(1) of the Constitution;

"communication"—

(a) in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—

(i) anything comprising speech, music, sounds, visual images or data of any description; and

(ii) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

(b) in relation to a postal operator or postal service (but not in the definition of "postal service"), includes anything transmitted by a postal service;

"communications data"—

(a) in relation to a telecommunications operator, telecommunications service or telecommunications system, has the meaning assigned by section 5(1); and

(b) in relation to a postal operator or postal service, has the meaning assigned by section 5(2);

"content" in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded; and

(b) anything which is systems data is not content;

"data" includes data which is not electronic data and any information (whether or not electronic);

"designated senior officer"—

(a) the Commissioner of Police;

(b) the Deputy Commissioner of Police;

(c) the head of the Financial Crimes Unit;

(d) a person for the time being lawfully exercising the functions of a person mentioned in paragraph *(a, (b))* or *(c)*;

"disclosure order" means an order made pursuant to section 50, to obtain disclosure of protected information in an intelligible form;

"Director of Public Prosecutions" means the Director of Public Prosecutions appointed under section 91(1) of the Constitution, and includes any person for the time being lawfully performing the functions of that office;

"electronic signature" means anything in electronic form which—

(a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

(b) is generated by the signatory or other source of the communication or data; and

(c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity or both;

"entity" means a person or thing;

"entity data" means any data which—

(a) is about—

(i) an entity;

(ii) an association between a telecommunications service and an entity; or

(iii) an association between any part of a telecommunication system and an entity;

(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location); and

(c) is not events data;

"events data" means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time;

"identifying data" means—

(a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service;

(b) data which may be used to identify, or assist in identifying, any event; or

(c) data which may be used to identify, or assist in identifying, the location of any person, event or thing,

and the reference to data which may be used to identify, or assist in identifying, any event includes—

(i) data relating to the fact of the event;

(ii) data relating to the type, method or pattern of event;

(iii) data relating to the time or duration of the event;

"intercept" and cognate expressions are to be construed (so far as it is applicable) in accordance with section 3;

"intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or a telecommunication network;

"interception device" means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus to intercept any communication but does not mean any instrument, device, equipment or apparatus, or any component thereof—

(a) furnished to the customer by a telecommunications operator in the ordinary course of business and being used by the customer in the ordinary course of his business;

(b) furnished by such customer for connection to the facilities of such telecommunications and being used by the customer in the ordinary course of business; or

(c) being used by a telecommunications operator in the ordinary course of business;

"internet connection record" means communications data which—

(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program; and

(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person);

"items subject to legal privilege" means—

(a) communications between an attorney-at-law and his client or any person representing his client made in connection with the giving of legal advice to the client;

(b) communications between an attorney-at-law and his client or any person representing his client or between such an adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings; and

(c) items enclosed with or referred to in such communications and made—

(i) in connection with the giving of legal advice; or

(ii) in connection with or in contemplation of legal proceedings and for the purposes of such proceedings,

when they are in the possession of a person who is entitled to possession of them, but items held with the intention of furthering a criminal purpose are not items subject to legal privilege;

"Judge" means a Judge of the Supreme Court;

"key" in relation to any electronic data, means any key, code, password, algorithm or other data the use of which, with or without keys—

(a) allow access to the electronic data; or

(b) facilitates the putting of the data into an intelligible form;

"lawful authority" has the meaning assigned by section 9;

"listed equipment" means any equipment declared to be listed equipment pursuant to section 66, and includes any component of such equipment;

"overseas authorities" means authorities of a country or territory outside the Islands;

"postal data" means data which—

(a) identifies, or purports to identify, any person, apparatus or location to or from which a communication is or may be transmitted;

(b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted;

(c) identifies, or purports to identify, the time at which an event relating to a communication occurs; or

(d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication;

and for the purposes of this definition "data", in relation to a postal item, includes anything written on the outside of the item;

"postal item" means—

(a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient; or

(b) any packet or parcel;

"postal operator" means a person providing a postal service to persons in the Islands.

"postal service" means a service that—

(a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the Islands or elsewhere) of postal items; and

(b) has as its main purpose, or one of its main purposes, to make available, or to facilitate, a means of transmission from place to place of postal items containing communications,

and also means a courier service, and reference to postal items shall be construed accordingly;

"private telecommunications system" means any telecommunication system which—

(a) is not a public telecommunication system;

(b) is attached, directly or indirectly, to a public telecommunication system(whether or not for the purposes of the communication in question); and

(c) includes apparatus which is both located in the Islands and used(with or without other apparatus) for making the attachment to that public telecommunication system;

"public postal service" means a postal service that is offered or provided to the public, or a substantial section of the public, in any one or more parts of the Islands;

"public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the Islands;

"public telecommunication system" means a telecommunication system located in the Islands—

(a) by means of which any public telecommunications service is provided; or

(b) which consists of parts of any other telecommunication system by means of which any such service is provided;

"related systems data", in relation to a warrant, means systems data relating to a relevant communication or to the sender or recipient, or intended recipient, of a relevant communication (whether or not a person);

"relevant communication", in relation to a warrant, means—

(a) any communication intercepted in accordance with the warrant in the course of its transmission by means of a postal service or telecommunications system; or

(b) any communication from which secondary data is obtained under the warrant;

"secondary data"—

(a) in relation to a communication transmitted by means of a postal service, means systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise);

(b) in relation to a communication transmitted by means of a telecommunication system, means—

(i) systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise);

(ii) identifying data which—

(A) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise);

(B) is capable of being logically separated from the remainder of the communication; and

(C) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication;

"source of journalistic information" means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used;

"systems data" means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following—

(a) a postal service;

(b) a telecommunication system (including any apparatus forming part of the system);

(c) any telecommunications service provided by means of a telecommunication system;

(d) a relevant system (including any apparatus forming part of the system);

(e) any service provided by means of a relevant system,

and a system is a "relevant system" if any communications or other information are held on or by means of the system;

"telecommunications operator" means a person who—

(a) offers or provides a telecommunications service to persons in the Islands; or

(b) controls or provides a telecommunication system which is (wholly or partly)—

(i) in the Islands; or

(ii) controlled from the Islands;

"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service), and the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system;

"telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the Islands or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy;

"terrorism" has the meaning assigned to that expression in the Prevention of Terrorism Ordinance;

"wireless telegraphy" has the meaning assigned by section 6;

"wireless telegraphy apparatus" has the meaning assigned by section 6.

(2) In this Ordinance, the interests of internal security shall be construed as including, but not limited to, the protection of the Islands from threats of sabotage, espionage, terrorism or subversion.

(3) For the purposes of this Ordinance detecting crime or serious crime is to be taken to include—

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime or (as the case may be) serious crime was committed, and

(b) the apprehension of the person by whom any crime or (as the case may be) serious crime was committed.

(4) For the purposes of subsection (3), "serious crime" means any offence specified in the Schedule.

Meaning of "interception"

3. (1) For the purposes of this Ordinance, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—

(a) the person does a relevant act in relation to the system; and

(b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

(2) For the purposes of determining whether a postal item is in the course of its transmission by means of a postal service—

(a) a postal packet shall be taken to be in course of transmission by means of a postal service from the time of its being delivered to any post office or post office letter box to the time of its being delivered to the addressee;

(b) the delivery of a postal packet of any description to a letter carrier or other person authorised to receive postal packets of that description for the post or to a person engaged in the business of a postal operator to be dealt with in the course of that business shall be a delivery to a post office; and

(c) the delivery of a postal packet—

(i) at the premises to which it is addressed or redirected, unless they are a post office from which it is to be collected;

(ii) to any box or receptacle to which the occupier of those premises has agreed that postal packets addressed to persons at those premises may be delivered; or

(iii) to the addressee's agent or to any other person considered to be authorised to receive the packet,

shall be a delivery to the addressee.

(4) For the purposes of this Ordinance, the interception of a communication is carried out in the Islands if, and only if—

(a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within the Islands; and

(b) the communication is intercepted—

(i) in the course of its transmission by means of a public telecommunication system or a public postal service; or

(ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in the Islands.

(5) In this section—

"relevant act", in relation to a telecommunication system, means—

(a) modifying, or interfering with, the system or its operation;

(b) monitoring transmissions made by means of the system;

(c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system;

"relevant time", in relation to a communication transmitted by means of a telecommunication system, means—

(a) any time while the communication is being transmitted; and

(b) any time when the communication is stored in or by the system (whether before or after its transmission).

(6) For the purposes of this section, references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—

(a) any part of the system; or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

(7) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.

Conduct that is not interception

4. (1) References in this Ordinance to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(2) References in this Ordinance to the interception of a communication in the course of its transmission by means of a postal service do not include references to—

(a) any conduct that takes place in relation only to so much of the communication as consists of any postal data comprised in, included as part of, attached to, or logically associated with a communication (whether by the sender or otherwise) for the purposes of any postal service by means of which it is being or may be transmitted; or

(b) any conduct, in connection with conduct falling within paragraph *(a)*, that gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying such postal data.

Meaning of "communication data"

5. (1) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service;

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted; or

(iii) does not fall within subparagraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within paragraph *(a)*(ii); or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator;

(ii) is about the architecture of a telecommunication system; and

(iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of paragraph *(b)* in the definition of "content", would be content of a communication.

(2) "Communications data", in relation to a postal operator or postal service, means—

(a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a postal service by means of which it is being or may be transmitted;

(b) information about the use made by any person of a postal service (but excluding any content of a communication (apart from information within paragraph *(a)*); or

(c) information not within paragraph *(a)* or *(b)* that is (or is to be or is capable of being) held or obtained by or on behalf of a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided.

Meaning of "wireless telegraphy" and "wireless telegraphy apparatus"

6. (1) "Wireless telegraphy" means the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for the purpose, of energy to which subsection (2) applies.

(2) This subsection applies to electromagnetic energy of a frequency not exceeding 3,000 gigahertz that—

(a) and serves for conveying messages, sound or visual images (whether or not the messages, sound or images are actually received by anyone), or for operating or controlling machinery or apparatus; or

(b) is used in connection with determining position, bearing or distance, or for gaining information as to the presence, absence, position or motion of an object or of a class of objects.

(3) "Wireless telegraphy apparatus" means apparatus for the emitting or receiving, over paths that are not provided by any

material substance constructed or arranged for the purpose, of energy to which subsection (2) applies.

PART II

PROHIBITIONS

Offence of unlawful interception

7. (1) A person commits an offence if—

(a) the person intentionally intercepts a communication in the course of its transmission by means of—

(i) a public telecommunication system;

(ii) a private telecommunication system; or

(iii) a public postal service;

(b) the interception is carried out in the Islands; and

(c) the person does not have lawful authority to carry out the interception.

(2) It is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—

(a) is a person with a right to control the operation or use of the system;

(b) has the express or implied consent of such a person to carry out the interception; or

(c) has lawful authority to carry out the interception.

(3) Section 9 contains provision about when a person has lawful authority to carry out an interception.

(4) A person who commits an offence under subsection (1) is liable on conviction on indictment to a fine or to a term of imprisonment of seven years, or to both.

(5) No proceedings for any offence which is an offence by virtue of this section may be instituted, except by or with the consent of the Director of Public Prosecutions.

(6) The court by which a person is convicted of an offence under this section may order that any device used to intercept a communication in the commission of the offence shall, unless subsection (7) applies, be forfeited to the Crown.

(7) This subsection applies where the device is listed equipment and the provisions of section 70 are to be followed.

Offence of unlawfully obtaining communications data

8. (1) A relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator commits an offence.

(2) In this section "relevant person" means—

(a) any person holding office under the Crown;

(b) any person employed by or for the purposes of the Royal Turks and Caicos Island Police Force; or

(c) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator.

(3) Subsection (1) does not apply to a relevant person who shows that the person acted in the reasonable belief that the person had lawful authority to obtain the communications data.

(4) A person who commits an offence under this section is liable on conviction on indictment to a fine of $50,000 or to a term of imprisonment for four years, or to both.

Lawful authority to carry out interception

9. (1) For the purposes of this Ordinance, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part III; or

(b) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is carried out in accordance with a targeted equipment interference warrant under Chapter 2 of Part III;

(ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property; or

(iii) is carried out in accordance with a court order made for that purpose;

(c) the sender and the intended recipient of the communication have each consented to its interception;

(d) if the communication is intercepted as an ordinary incident to the provision of public postal services

or telecommunications services or to the enforcement of any law in force in the Islands relating to the use of those services;

(e) if the interception is of a communication made through a telecommunications system that is so configured as to render the communication readily accessible to the general public;

(f) if the interception is of a communication transmitted and received within an internal or private network and is done by a person who has—

(i) a right to control the operation or use of the network; or

(ii) the express or implied consent of a person referred to in subparagraph (i);

(2) Conduct which has lawful authority for the purposes of this Ordinance by virtue of subsection (1)*(a)* or *(b)* is to be treated as lawful for all other purposes.

PART III

LAWFUL INTERCEPTION OF COMMUNICATIONS

Chapter 1

INTERCEPTION WARRANTS

Warrants that may be issued under this Chapter

10. (1) There are two kinds of warrants that may be issued under this Chapter—

(a) targeted interception warrant; and

(b) mutual assistance warrant.

(2) A targeted interception warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—

(a) the interception, in the course of its transmission by means of a postal service or telecommunications system, of communications described in the warrant;

(b) the obtaining of secondary data from communications transmitted by means of a postal

service or telecommunications system and described in the warrant; and

(c) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(3) A mutual assistance warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—

(a) the making of a request, in accordance with an international mutual assistance agreement, for the provision of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;

(b) the provision to the competent authorities of a country or territory outside the Islands, in accordance with such an agreement, of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;

(c) the disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(4) A targeted interception warrant or mutual assistance warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including—

(i) the interception of communications not described in the warrant; and

(ii) conduct for obtaining secondary data from such communications;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant;

(c) any conduct for obtaining related systems data from any postal operator or telecommunications operator.

Obtaining secondary data

11. (1) This section has effect for the purposes of this Part.

(2) In relation to a communication transmitted by means of a postal service, references to obtaining secondary data from the communication are references to obtaining such data in the course of the transmission of the communication.

(3) In relation to a communication transmitted by means of a telecommunication system, references to obtaining secondary data from the communication are references to obtaining such data—

(a) while the communication is being transmitted; or

(b) at any time when the communication is stored in or by the system (whether before or after its transmission).

Subject-matter of warrant

12. (1) A warrant under this Chapter may relate to—

(a) a particular person or organisation; or

(b) a single set of premises.

(2) In addition, a targeted interception warrant may relate to—

(a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;

(b) more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation.

Power of Judge to issue warrant

13. (1) Subject to the provisions of this section, a Judge may, on application made by the Director of Public Prosecutions, on behalf of an authorised officer, issue a targeted interception warrant or a mutual assistance warrant if—

(a) the Judge considers that the warrant is necessary on grounds falling within section 14;

(b) the Judge considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct;

(c) the Judge considers that satisfactory arrangements made for the purposes of sections 40 and 41 are in force in relation to the warrant;

(d) subject to section 15(1), the application is in writing and supported by an affidavit; and

(e) the Judge considers that, where applicable, all requirements set out within sections 16 to 18 have been met.

(2) The records relating to every application for a targeted interception warrant or mutual assistance warrant, or the renewal or modification thereof shall be—

(a) placed in a packet and sealed by the Judge to whom the application is made immediately on determination of the application; and

(b) kept in the custody of the court in a place to which the public has no access or such other place as the Judge may authorise.

(3) The records referred to in subsection (2), may only be opened by order of a Judge.

(4) All applications for a targeted interception warrant or a mutual assistance warrant shall be made *ex parte* and heard by the Judge in Chambers.

(5) A Judge in considering an application for a warrant may require the authorised officer to furnish such further information as the Judge thinks fit.

Grounds on which warrant may be issued by Judge

14. (1) This section has effect for the purposes of this Part.

(2) A targeted interception warrant is necessary on grounds falling within this section if it is necessary—

(a) in the interests of internal security;

(b) for the prevention or detection of any offences specified in the Schedule; or

(c) in the interests of the economic well-being of the Islands so far as those interests are also relevant to the interests of internal security.

(3) A mutual assistance warrant is necessary on grounds falling within this section if—

(a) it is necessary for the purpose of giving effect to the provisions of an international mutual assistance agreement; and

(b) the circumstances appear to the Judge to be equivalent to those in which the Judge would issue a warrant by virtue of subsection (2)*(b)*.

(4) A warrant may be considered necessary as mentioned in subsection (2)*(c)* only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the Islands.

(5) A warrant may not be considered necessary on grounds falling within this section if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(6) Without prejudice to the generality of the wording in subsection (2)*(a)*, this requirement will be met if the Judge is satisfied that a serious offence has been or is being or will probably be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime.

Issue of warrant in urgent cases

15. (1) Where a Judge is satisfied that the urgency of the circumstances so requires he may dispense with the requirements specified in section 13(1)*(d)* and proceed to hear an oral application made by the Director of Public Prosecutions on behalf of an authorised officer for a targeted interception warrant or a mutual assistance warrant.

(2) A Judge may, on an oral application made to him pursuant to subsection (1), issue a targeted interception warrant or a mutual assistance warrant, if he is satisfied that—

(a) he would have issued the warrant under section 13 if the substance of the oral submissions made to him had been contained within the documentation specified in section 13(1)*(d)*; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, for the Director of Public Prosecutions to comply with section 13(1)*(d)*.

(3) A warrant issued in accordance with this section shall have the same scope as a warrant issued pursuant to section 13.

(4) Where a warrant is issued under this section, the Director of Public Prosecutions may, on behalf of the authorised officer, within seventy-two hours of the time of its issue, submit to a Judge a written application and affidavit in accordance with the provisions of section 13(1)*(d)*.

(5) On receipt of an application made pursuant to subsection (4), the Judge shall—

(a) determine the application in accordance with section 13; and

(b) cancel the warrant issued under this section.

(6) A warrant issued under this section shall expire and cease to be of effect at the expiry of seventy-two hours after the time at which it was issued unless it is cancelled before that time in accordance with subsection (5)*(b)*.

(7) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant before it ceases to have effect;

(b) if anything is in the process of being done under the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped; or

(ii) anything done which it is not reasonably practicable to stop.

Items subject to legal privilege

16. (1) Subsections (2) to (5) apply if—

(a) an application is made under section 13(1) for a targeted interception warrant or mutual assistance warrant; and

(b) the purpose, or one of the purposes of the warrant is to authorise or require the interception of items subject to legal privilege.

(2) The application shall contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require the interception of items subject to legal privilege.

(3) In deciding whether to issue the warrant, the Judge shall have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The Judge to whom the application is made may issue the warrant only if he considers—

(a) that there are exceptional and compelling circumstances that make it necessary to authorise or require the interception of items subject to legal privilege; and

(b) that arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of such items.

(5) The warrant may not be issued if it is considered necessary only as mentioned in section 14(2)*(c)*.

(6) For the purposes of subsection (4)*(a)*, there cannot be exceptional and compelling circumstances that make it necessary to authorise or require the interception of items subject to legal privilege unless—

(a) the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to legal privilege;

(b) there are no other means by which the information may reasonably be obtained; and

(c) in the case of a warrant considered necessary as mentioned in section 14(2)*(b)* or (3), obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if—

(a) an application is made under section 13(1) for a targeted interception warrant or mutual assistance warrant;

(b) the authorised officer considers that the relevant communications are likely to include items subject to legal privilege; and

(c) subsections (2) to (5) do not apply.

(8) The application shall contain—

(a) a statement that the authorised officer considers that the relevant communications are likely to include items subject to legal privilege; and

(b) an assessment of how likely it is that the relevant communications will include such items.

(9) The Judge may issue the warrant only if he considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section "relevant communications" means any communications the interception of which is authorised or required by the warrant.

(11) Subsections (12) and (13) apply if—

(a) an application is made under section 13(1) for a targeted interception warrant or mutual assistance warrant;

(b) the purpose, or one of the purposes, of the warrant is to authorise or require the interception of

communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege; and

(c) the authorised officer considers that the communications ("the targeted communications") are likely to be communications made with the intention of furthering a criminal purpose.

(12) The application shall—

(a) contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require the interception of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege; and

(b) set out the reasons for believing that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

(13) The Judge may issue the warrant only if he considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

Confidential journalistic material

17. (1) This section applies where—

(a) an application is made under section 13(1) for a targeted interception warrant or mutual assistance warrant; and

(b) the purposes, or one of the purposes of the warrant is to authorise or require the interception of communications which the authorised officer believes will be communications containing confidential journalistic material.

(2) The application shall contain a statement that the purpose, or one of the purposes of the warrant is to authorise or require the interception of communications which the authorised officer believes will be communications containing confidential journalistic material.

(3) The Judge to whom the application is made may issue the warrant only if he considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material.

(4) For the purposes of this Ordinance, "journalistic material" means material created or acquired for the purposes of journalism.

(5) For the purposes of this section, where—

(a) a person ("R") receives material from another person ("S"); and

(b) S intends R to use the material for the purposes of journalism, R is to be taken to have acquired it for those purposes.

Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.

(6) For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person.

(7) For the purposes of this section—

(a) material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose; and

(b) material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.

(8) For the purposes of this Ordinance, "confidential journalistic material" means—

(a) in the case of material contained in a communication, journalistic material which the sender of the communication—

(i) holds in confidence; or

(ii) intends the recipient, or intended recipient, of the communication to hold in confidence;

(b) in any other case, journalistic material which a person holds in confidence.

(9) A person holds material in confidence for the purposes of this section if—

(a) the person holds it subject to an express or implied undertaking to hold it in confidence; or

(b) the person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment.

Sources of journalistic material

18. (1) This section applies where—

(a) an application is made under section 13(1) for a targeted interception warrant or mutual assistance warrant; and

(b) the purpose, or one of the purposes of the warrant is to identify or confirm a source of journalistic information.

(2) The application shall contain a statement that the purpose or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(3) The Judge to whom the application is made may issue the warrant only if the Judge considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of communications that identify sources of journalistic information.

Requirements that must be met by warrant

19. (1) A warrant under this Chapter shall contain a provision stating whether it is a targeted interception warrant or a mutual assistance warrant.

(2) A warrant issued under this Chapter shall be addressed to the authorised officer on whose behalf the Director of Public Prosecutions made the application for the warrant.

(3) A warrant that relates to a particular person or organisation, or to a single set of premises, shall name or describe that person or organisation or those premises.

(4) A warrant that relates to a group of persons who share a common purpose or who carryon (or may carry on) a particular activity shall—

(a) describe that purpose or activity; and

(b) name or describe as many of those persons as it is reasonably practicable to name or describe.

(5) A warrant that relates to more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation, shall—

(a) describe the investigation or operation; and

(b) name or describe as many of those persons or organisations, or as many of those sets of premises, as it is reasonably practicable to name or describe.

(6) Where a targeted interception warrant or mutual assistance warrant authorises or requires the interception of communications described in the warrant, or the obtaining of secondary data from such communications, the warrant shall specify the addresses, numbers, apparatus, or other factors, or combination of factors, that are to be used for identifying the communications.

(7) Any factor, or combination of factors, specified in accordance with subsection (6), shall be one that identifies communications which are likely to be or to include—

(a) communications from, or intended for, any person or organisation named or described in the warrant; or

(b) communications originating on, or intended for transmission to, any premises named or described in the warrant.

(8) In this section any reference to communications from, or intended for, a person or organisation includes communications from, or intended for, anything owned, controlled or operated by that person or organisation.

(9) A targeted interception warrant or mutual assistance warrant may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Ordinance.

(10) A targeted interception warrant or mutual assistance warrant may specify conditions or restrictions relating to the interception of communications authorised therein.

(11) In this section "address" includes a location, e-mail address, telephone number or other number or designation used for the purpose of identifying telecommunications systems or apparatus.

Duration of warrant

20. (1) A warrant under this Chapter ceases to have effect at the end of the relevant period, unless—

(a) it is renewed before the end of that period;

(b) it is cancelled or otherwise ceases to have effect before the end of that period; or

(c) it is a warrant issued in an urgent case.

(2) In this section "relevant period" means a period of six months beginning with—

(a) the day on which the warrant was issued; or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) The duration of a warrant issued in an urgent case is specified in section 15(6).

Renewal of warrant

21. (1) If the renewal conditions are met, a Judge may renew a targeted interception warrant or mutual assistance warrant at any time during the renewal period.

(2) The renewal conditions are—

(a) an application for renewal has been made by the Director of Public Prosecutions on behalf of an authorised officer;

(b) the application is in writing and accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal of the warrant;

(c) the Judge considers that the warrant continues to be—

(i) necessary on any relevant grounds; and

(ii) proportionate to what is sought to be achieved by that conduct;

(d) the Judge considers that satisfactory arrangements made for the purposes of sections 40 and 41 are in force in relation to the warrant;

(e) the Judge considers that, where applicable, all requirements set out within sections 16 to 18 have been met.

(3) In subsection (2)*(c)*(i), "relevant grounds" means grounds specified in section 14(2) or (3).

(4) In this section, "the renewal period" means the period of thirty days ending with the day at the end of which the warrant would otherwise cease to have effect.

(5) This section does not apply to warrants issued in urgent cases, pursuant to section 15.

Chapter 2

EQUIPMENT INTERFERENCE

Meaning of "equipment data"

22. (1) In this Chapter, "equipment data" means—

(a) systems data;

(b) data which falls within subsection (2).

(2) The data falling within this subsection is identifying data which—

(a) is, for the purposes of a relevant system, comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information;

(b) is capable of being logically separated from the remainder of the communication or the item of information; and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact.

(3) In subsection (2), "relevant system" means any system on or by means of which the data is held.

Warrant under this Chapter: targeted equipment interference warrant

23. (1) A targeted equipment interference warrant may be issued under this Chapter.

(2) A targeted equipment interference warrant is a warrant which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—

(a) communications;

(b) equipment data;

(c) any other information.

(3) A targeted equipment interference warrant—

(a) shall also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;

(b) may also authorise that person to secure the disclosure, in any manner described in the warrant, of anything obtained under the warrant by virtue of paragraph *(a)*.

(4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by—

(a) monitoring, observing or listening to a person's communications or other activities;

(b) recording anything which is monitored, observed or listened to.

(5) A targeted equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) A targeted equipment interference warrant may not, by virtue of subsection (3),authorise or require a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 7(1).

(7) Subsection (5)*(a)* does not authorise a person to engage in conduct which could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system (whether before or after its transmission).

(9) Any conduct which is carried out in accordance with a warrant under this Part is lawful for all purposes.

Subject matter of targeted equipment interference warrant

24. A targeted equipment interference warrant may relate to any one or more of the following matters—

(a) equipment belonging to, used by or in the possession of a particular person or organisation;

(b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;

(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;

(d) equipment in a particular location;

(e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;

(f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;

(g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;

(h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

Power of Judge to issue targeted equipment interference warrant

25. (1) Subject to the provisions of this section, a Judge may, on application made by the Director of Public Prosecutions, on behalf of an authorised officer, issue a targeted equipment interference warrant if—

(a) the Judge considers that the warrant is necessary on grounds falling within subsection (2);

(b) the Judge considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct;

(c) the Judge considers that satisfactory arrangements made for the purposes of sections 40 and 41 are in force in relation to the warrant;

(d) subject to section 26(1), the application is in writing and supported by an affidavit; and

(e) the Judge considers that, where applicable, all requirements set out within sections 27 to 29 have been met.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of internal security;

(b) for the prevention or detection of any offences specified in the Schedule; or

(c) in the interests of the economic well-being of the Islands so far as those interests are also relevant to the interests of internal security.

(3) A warrant may be considered necessary as mentioned in subsection (2)*(c)* only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the Islands.

(4) A warrant may not be considered necessary on grounds falling within this section if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(5) Without prejudice to the generality of the wording in subsection (2)*(a)*, this requirement will be met if the Judge is satisfied that a serious offence has been or is being or will probably be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime.

(6) The records relating to every application for a targeted equipment interference warrant or the renewal or modification thereof shall be—

(a) placed in a packet and sealed by the Judge to whom the application is made immediately on determination of the application; and

(b) kept in the custody of the court in a place to which the public has no access or such other place as the Judge may authorise.

(7) The records referred to in subsection (6), may only be opened by order of a Judge.

(8) All applications for a targeted equipment interference warrant shall be made *ex parte* and heard by the Judge in Chambers.

(9) A Judge in considering an application for a warrant may require the authorised officer to furnish such further information as the Judge thinks fit.

Issue of targeted equipment interference warrant in urgent cases

26. (1) Where a Judge is satisfied that the urgency of the circumstances so requires he may dispense with the requirements specified in section 25(1)*(d)* and proceed to hear an oral application made by the Director of Public Prosecutions on behalf of an authorised officer for a targeted equipment interference warrant.

(2) A Judge may, on an oral application made to him pursuant to subsection (1), issue a targeted equipment interference warrant, if he is satisfied that—

(a) he would have issued the warrant under section 25 if the substance of the oral submissions made to him had been contained within the documentation specified in section 25(1)*(d)*; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, for the Director of Public Prosecutions to comply with section 25(1)*(d)*.

(3) A warrant issued in accordance with this section shall have the same scope as a warrant issued pursuant to section 25.

(4) Where a warrant is issued under this section, the Director of Public Prosecutions may, on behalf of the authorised officer, within seventy-two hours of the time of its issue, submit to a Judge a written application and affidavit in accordance with the provisions of section 25(1)*(d)*.

(5) On receipt of an application made pursuant to subsection (4), the Judge shall—

(a) determine the application in accordance with section 25; and

(b) cancel the warrant issued under this section.

(6) A warrant issued under this section shall expire and cease to be of effect at the expiry of seventy-two hours after the time at which it was issued unless it is cancelled before that time in accordance with subsection (5)*(b)*.

(7) Nothing in this section affects the lawfulness of—

(a) anything done under the warrant before it ceases to have effect;

(b) if anything is in the process of being done under the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped; or

(ii) anything done which it is not reasonably practicable to stop.

Items subject to legal privilege: application for targeted equipment interference warrant

27. (1) Subsections (2) to (5) apply if—

(a) an application is made under section 25(1) for a targeted equipment interference warrant; and

(b) the purpose, or one of the purposes of the warrant is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege.

(2) The application shall contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege.

(3) In deciding whether to issue the warrant, the Judge shall have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The Judge to whom the application is made may issue the warrant only if he considers—

(a) that there are exceptional and compelling circumstances that make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege; and

(b) that arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of such items.

(5) The warrant may not be issued if it is considered necessary only as mentioned in section 25(2)*(c)*.

(6) For the purposes of subsection (4)*(a)*, there cannot be exceptional and compelling circumstances that make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege unless—

(a) the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to legal privilege;

(b) there are no other means by which the information may reasonably be obtained; and

(c) in the case of a warrant considered necessary as mentioned in section 25(2)*(b)*, obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if—

(a) an application is made under section 25(1) for a targeted equipment interference warrant; and

(b) the authorised officer considers that the relevant material is likely to include items subject to legal privilege; and

(c) subsections (2) to (5) do not apply.

(8) The application shall contain—

(a) a statement that the applicant considers that the relevant material is likely to include items subject to legal privilege; and

(b) an assessment of how likely it is that the relevant communications will include such items.

(9) The Judge may issue the warrant only if he considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section "relevant material" means any material the interception of which is authorised or required by the warrant.

(11) Subsections (12) and (13) apply if—

(a) an application is made under section 25(1) for a targeted equipment interference warrant;

(b) the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege; and

(c) the authorised officer considers that the communications or the other items of information ("the targeted communications or other items of information") are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(12) The application shall—

(a) contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege; and

(b) set out the reasons for believing that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(13) The Judge may issue the warrant only if he considers that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

Confidential journalistic material: application for targeted equipment interference warrant

28. (1) This section applies where—

(a) an application is made under section 25(1) for a targeted equipment interference warrant; and

(b) the purposes, or one of the purposes of the warrant is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the authorised officer believes will be communications or other items of information containing confidential journalistic material.

(2) The application shall contain a statement that the purpose, or one of the purposes of the warrant is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the

authorised officer believes will be communications or other items of information containing confidential journalistic material.

(3) The Judge to whom the application is made may issue the warrant only if he considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of communications or other items of information containing confidential journalistic material.

(4) For the meaning of meaning of "journalistic material" and "confidential journalistic material" see section 17(4) and (8).

Sources of journalistic material: application for targeted equipment interference warrant

29. (1) This section applies where—

(a) an application is made under section 25(1) for a targeted equipment interference warrant; and

(b) the purpose, or one of the purposes of the warrant is to identify or confirm a source of journalistic information.

(2) The application shall contain a statement that the purpose or one of the purposes, of the warrant is to identify or confirm a source of journalistic information.

(3) The Judge to whom the application is made may issue the warrant only if the Judge considers that the arrangements made for the purposes of section 40 include specific arrangements for the handling, retention, use and destruction of communications or other items of information that identify sources of journalistic information.

Requirements that must be met by targeted equipment interference warrant

30. (1) A warrant under this Chapter shall contain a provision stating that it is a targeted equipment interference warrant.

(2) A warrant issued under this Chapter shall be addressed to the authorised officer on whose behalf the Director of Public Prosecutions made the application for the warrant.

(3) In the case of a targeted equipment interference warrant which relates to a matter described in the first column of the Table below, the warrant shall include the details specified in the second column.

Matter	*Details to be included in the warrant*
Equipment belonging to, used by or in the possession of a particular person or organisation	The name of the person or organisation or a description of the person or organisation
Equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe
Equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe
Equipment in a particular location	A description of the location
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe
Equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description	A description of the particular activity or activities
Equipment which is being, or maybe, used to test, maintain or develop capabilities relating to interference with equipment	A description of the nature of the testing, maintenance or development of capabilities
Equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, interference with equipment	A description of the nature of the training

(4) A targeted equipment interference warrant shall also describe—

(a) the type of equipment which is to be interfered with; and

(b) the conduct which the person to whom the warrant is addressed is authorised to take.

(5) A targeted equipment interference warrant may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Ordinance.

(6) A targeted equipment interference warrant may specify conditions or restrictions relating to the interference with equipment for the purpose of obtaining communications or other items of information.

Duration of targeted equipment interference warrant

31. (1) A warrant under this Chapter ceases to have effect at the end of the relevant period, unless—

(a) it is renewed before the end of that period;

(b) it is cancelled or otherwise ceases to have effect before the end of that period; or

(c) it is a warrant issued in an urgent case.

(2) In this section "relevant period" means a period of six months beginning with—

(a) the day on which the warrant was issued; or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) The duration of a warrant issued in an urgent case is specified in section 26(6).

Renewal of targeted equipment interference warrant

32. (1) If the renewal conditions are met, a Judge may renew a targeted equipment interference warrant at any time during the renewal period.

(2) The renewal conditions are—

(a) an application for renewal has been made by the Director of Public Prosecutions on behalf of an authorised officer;

(b) the application is in writing and accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal of the warrant;

(c) the Judge considers that the warrant continues to be—

(i) necessary on any relevant grounds;

(ii) proportionate to what is sought to be achieved by that conduct;

(d) the Judge considers that satisfactory arrangements made for the purposes of sections 40 and 41 are in force in relation to the warrant;

(e) the Judge considers that, where applicable, all requirements set out within sections 27 to 29 have been met.

(3) In subsection (2)*(c)*(i), "relevant grounds" means grounds specified in section 25(2).

(4) In this section, "the renewal period" means the period of thirty days ending with the day at the end of which the warrant would otherwise cease to have effect.

(5) This section does not apply to warrants issued in urgent cases, pursuant to section 26.

Chapter 3

MODIFICATION AND CANCELLATION OF WARRANTS AND REPORT

Modification of warrant

33. (1) This section applies to all warrants issued under this Part, except warrants issued in cases of urgency under sections 15 and 26.

(2) If the relevant conditions in subsection (3) are met, a Judge may modify the provisions of a warrant at any time.

(3) The relevant conditions are—

(a) an application for modification of the warrant has been made by the Director of Public Prosecutions on behalf of an authorised officer;

(b) the application is in writing and accompanied by an affidavit deposing to the circumstances relied on as justifying the modification of the warrant;

(c) the Judge considers that the modification is—

(i) necessary; and

(ii) proportionate to what is sought to be achieved by that conduct.

(4) The only modifications that may be made under this section are—

(a) adding, varying or removing the name or description of a person, organisation or set of premises to which the warrant relates; and

(b) adding, varying or removing anything specified in the warrant in accordance with section 19(3), (4), (5) or (6), and section 30(3) or (4).

(5) A Judge may also modify the provisions of a warrant in the circumstances prescribed by section 35(3).

Cancellation of warrant

34. (1) This section applies to all warrants issued under this Part.

(2) If the authorised officer considers that—

(a) a warrant is no longer necessary; or

(b) the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,

the authorised officer shall ensure that the Director of Public Prosecutions is provided with this information as soon as reasonably practicable.

(3) On receipt of the information specified in subsection (2), the Director of Public Prosecutions shall apply to a Judge in writing for the warrant to be cancelled.

(4) On receipt of the application specified in subsection (3) the Judge shall cancel the warrant.

(5) Where a warrant has been cancelled—

(a) the Director of Public Prosecutions shall forthwith notify the authorised officer concerned of the cancellation; and

(b) on receipt of this notification, the authorised officer shall, as far as is reasonably practicable, secure that anything in the process of being done under that warrant stops as soon as possible.

(6) A warrant that has been cancelled under this section may not be renewed.

(7) A Judge may also cancel a warrant in the circumstances prescribed by section 35(3).

Report on progress

35. (1) This section applies to all warrants issued under this Part, except warrants issued in cases of urgency under sections 15 and 26.

(2) A Judge who has issued a warrant, may at the issuance, or at any stage before the date of expiry thereof, in writing require the authorised officer on whose behalf either application was made in respect of the warrant to report to him in writing at such intervals as he determines on—

(a) the progress that has been made towards achieving the objectives of the warrant; and

(b) any other matter which the Judge deems necessary.

(3) A Judge may take one of the actions specified in subsection (4) if—

(a) the authorised officer fails to provide a report required by subsection (2); or

(b) the contents of a report provided in accordance with subsection (2) are such that the Judge considers that one of the actions specified in subsection (4) is required.

(4) The actions referred to in subsection (3) are—

(a) modification of the warrant in a manner specified by section 33(4); or

(b) cancellation of the warrant in accordance with section 34.

Chapter 4

IMPLEMENTATION OF WARRANTS

Implementation of warrant

36. (1) This section applies to all warrants issued under this Part.

(2) In giving effect to a warrant to which this section applies, the authorised officer may (in addition to acting alone) act through, or together with, such other persons as are identified in the warrant as being required to provide assistance in giving effect to the warrant.

(3) For the purpose of requiring any person to provide assistance in relation to a warrant to which this section applies, the authorised officer shall—

(a) serve a copy of the warrant on any person who is identified in the warrant as being required to provide such assistance; or

(b) make arrangements for the service of a copy of the warrant on any such person.

(4) For the purposes of this Ordinance, the provision of assistance in giving effect to a warrant to which this section applies includes any disclosure to the authorised officer, or to persons acting on behalf of the authorised officer, of anything obtained under the warrant.

(5) References in this section and sections 37 and 38 to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant; and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Service of warrant

37. (1) This section applies to the service of a warrant under section 36(3).

(2) A copy of the warrant must be served in such a way as to bring the contents of the warrant to the attention of the person who is identified as being required to provide assistance in relation to it.

Duty of operator to assist with implementation

38. (1) Subject to subsection (3), where a relevant operator—

(a) is identified in a warrant issued under this Part as being required to provide assistance; and

(b) is served with a copy of that warrant in accordance with section 37,

that person shall without delay provide all assistance required of him for giving effect to that warrant.

(2) The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take.

(3) In carrying out the steps required by subsection (1) the relevant operator shall ensure that the assistance is rendered—

(a) as unobtrusively; and

(b) with minimum interference to the services that such a person or entity normally provides to the party affected by the warrant,

as can reasonably be expected in the circumstances.

(4) In this section "relevant operator" means a postal operator or a telecommunications operator.

(5) A person who knowingly fails to comply with subsection (1) commits an offence and liable on summary conviction to a fine of $10,000 or to a term of imprisonment of six months, or to both.

Further provisions relating to postal articles

39. If any postal article has been taken into possession pursuant to section 36(2), the authorised officer who implements the warrant or assists with the implementation thereof—

(a) shall take proper care of the postal article and may, if the postal article concerned is perishable, with due regard to the interests of the persons concerned, dispose of that postal article in such manner as circumstances may require;

(b) shall retain the postal article, if it has not been disposed of in terms of paragraph *(a)*, or cause it to be returned to the postal operator if, in the opinion of the authorised officer—

(i) no criminal or civil proceedings as contemplated will be instituted in connection with the postal article; or

(ii) the postal article will not be required for any purposes at ongoing criminal or civil proceedings; and

(iii) such postal article may be returned without prejudice to the internal security of the Islands, as the case may be.

Chapter 5

CONFIDENTIALITY AND SAFEGUARDS

Safeguards relating to retention and disclosure of material

40. (1) The authorised officer shall ensure, in relation to every warrant issued under this Part, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant.

(2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(3) For the purposes of this section something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary on any of the grounds falling within section 14 or section 25(2) on which a warrant under this Part may be necessary;

(b) it is necessary for facilitating the carrying out of any functions under this Ordinance of an authorised officer or the Director of Public Prosecutions;

(c) it is necessary for facilitating the carrying out of any functions under this Ordinance of a Judge;

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it.

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, on any of the grounds falling within section 14 or section 25(2) on which a warrant under this Part may be necessary;

(b) its retention is not necessary for any of the purposes mentioned in subsection (3)*(b)* to *(d)*.

(7) Where—

(a) a communication which has been intercepted in accordance with a targeted interception warrant or mutual assistance warrant is retained, following its examination, for purposes other than the destruction of the communication; or

(b) material obtained under a targeted equipment interference warrant is retained, for purposes other than the destruction of the material; and

(c) it is a communication that contains confidential journalistic material or identifies a source of journalistic information,

the authorised officer must inform the Judge as soon as is reasonably practicable.

(8) A Judge, on receiving information from an authorised officer pursuant to subsection (7), may proceed in the same manner as if he had required a report, in accordance with section 35(2), and the authorised officer had provided that information in response to that requirement.

(9) Subsection (10) applies if—

(a) any material obtained under the warrant has been handed over to any overseas authorities; or

(b) a copy of any such material has been given to any overseas authorities.

(10) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (9)*(a)*, or to the copy mentioned in subsection (9)*(b)*, the arrangements made for the purposes of this section are not required to secure that those requirements are met.

(11) In this section "copy", in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant; and

(b) any record which—

(i) refers to any interception or to the obtaining of any material; and

(ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates; or

(iii) is a record of the identities of persons who owned, used or were in possession of the equipment which was interfered with to obtain that material,

and "copied" is to be read accordingly.

Safeguards relating to disclosure of material overseas

41. (1) The authorised officer shall ensure, in relation to every warrant issued under this Part, that arrangements are in force for securing that—

(a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met; and

(b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the authorised officer—

(a) that requirements corresponding to the requirements of section 40(2) and (5) will apply, to such extent (if any) as the authorised officer considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question; and

(b) that restrictions are in force which would prevent, to such extent (if any) as the authorised officer considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the Islands which would result in a prohibited disclosure.

(3) In subsection (2)*(b)* "prohibited disclosure" means a disclosure which, if made in the Islands, would breach the prohibition in section 44(1).

(4) In this section "copy" has the same meaning as in section 40.

Additional safeguards for items subject to legal privilege

42. (1) This section applies where an item subject to legal privilege which has been intercepted in accordance with a targeted interception warrant or mutual assistance warrant, or obtained under a targeted equipment interference warrant, is retained, following its examination, for purposes other than the destruction of the item.

(2) The authorised officer shall inform a Judge of the retention of the item as soon as is reasonably practicable.

(3) Unless a Judge considers that subsection (5) applies to the item, the Judge shall—

(a) direct that the item is destroyed; or

(b) impose one or more conditions as to the use or retention of that item.

(4) If a Judge considers that subsection (5) applies to the item, the Judge may nevertheless impose such conditions under subsection (3)*(b)* as the Judge considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if—

(a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege; and

(b) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury.

Failure to destroy material

43. (1) A person commits an offence if—

(a) any of the provision of sections 40 or 42, or any direction or order made under those provisions, places an obligation on that person to destroy material obtained under a targeted interception warrant or a mutual assistance warrant; and

(b) that person fails without reasonable excuse to destroy that material.

(2) A person who commits an offence under this section is liable on summary conviction to a fine of $40,000 or to a term of imprisonment for two years, or to both.

Exclusion of matters from legal proceedings

44. (1) No evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which, in any manner—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—

(i) any content of an intercepted communication; or

(ii) any secondary data obtained from a communication; or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

(2) In this section "interception-related conduct" means—

(a) conduct by a person within subsection (3) that is, or in the absence of any lawful authority would be, an offence under section 7(1);

(b) the making of an application by any person for, or the issue of, a targeted interception warrant or mutual assistance warrant;

(c) the imposition of any requirement on any person to provide assistance in giving effect to a targeted interception warrant or mutual assistance warrant.

(3) The persons referred to in subsection (2)*(a)* are—

(a) any person to whom a targeted interception warrant or a mutual assistance warrant issued pursuant to this Ordinance may be addressed;

(b) any person holding office under the Crown;

(c) any person employed by or for the purposes of the Royal Turks and Caicos Island Police Force;

(d) any postal operator or telecommunications operator;

(e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator.

Exceptions to section 44

45. (1) Section 44(1) does not prohibit the disclosure of any content of a communication, or secondary data obtained from a communication, if the interception of that communication was lawful by virtue of any section 9(1)*(b)* to *(f)*.

(2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by subsection (1), section 44(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

(3) Section 44(1)*(b)* does not prohibit the doing of anything that discloses any conduct of a person for which that person has been convicted of an offence under section 7(1), 38(5) or 48(1).

(4) Section 44(1) does not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the fairness or unfairness of a dismissal on the grounds of any conduct constituting an offence under section 7(1), 38(5) or 48(1).

(5) Section 44(1) does not apply in relation to any proceedings for a relevant offence.

(6) For the purpose of this section "relevant offence" means—

(a) an offence under any provision of this Ordinance;

(b) an offence under section 7, 15 or 54 of the Telecommunications Ordinance;

(c) perjury in the course of any proceedings mentioned in subsection (4);

(d) attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the proceeding paragraphs;

(e) contempt of court committed in the course of, or in relation to, any proceedings mentioned in subsection (4).

(7) Nothing in section 44(1) prohibits—

(a) a disclosure to a person ("P") conducting a criminal prosecution that is made for the purpose only of enabling P to determine what is required of P by P's duty to secure the fairness of the prosecution; or

(b) a disclosure to a relevant judge in a case in which the judge has ordered the disclosure to be made to the judge alone.

(8) A Judge may order a disclosure under subsection (1)*(b)* only if the judge considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(9) Where in criminal proceedings—

(a) a Judge orders a disclosure under subsection (1)*(b)*; and

(b) in consequence of that disclosure, the judge considers that there are exceptional circumstances requiring the judge to make a direction under this subsection,

the judge may direct the person conducting the prosecution to make for the purposes of the proceedings any admission of fact which the judge considers essential in the interests of justice.

(10) Nothing in any direction under subsection (9) may authorise or require anything to be done in contravention of section 44(1).

Duty not to make unauthorised disclosures

46. (1) A person to whom this section applies shall not make an unauthorised disclosure to another person.

(2) A person makes an unauthorised disclosure for the purposes of this section if—

(a) the person discloses any of the matters within subsection (4) in relation to a warrant under this Part; and

(b) the disclosure is not an excepted disclosure.

(3) This section applies to the following persons—

(a) an authorised officer;

(b) any person holding office under the Crown;

(c) any person employed by, or for the purposes of, the Royal Turks and Caicos Island Police Force;

(d) any postal operator or telecommunications operator;

(e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator;

(f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a targeted interception warrant or mutual assistance warrant.

(4) The matters referred to in subsection (2)*(a)* are—

(a) the existence or contents of the warrant;

(b) the details of the issue of the warrant or of any renewal or modification of the warrant;

(c) the existence or contents of any requirement to provide assistance in giving effect to the warrant;

(d) the steps taken in pursuance of the warrant or of any such requirement;

(e) in relation to any warrant issued under Chapter 1 of this Part, any of the material obtained under the warrant;

(f) in relation to a warrant issued under Chapter 2 of this Part, any of the material obtained under the warrant in a form which identifies it as having been obtained under a warrant under Chapter 2.

Section 46: meaning of "excepted disclosure"

47. (1) For the purposes of section 46 a disclosure made in relation to a warrant is an "excepted disclosure" if it falls within any of the Heads set out in subsection (2), (3), (4) or (5).

(2) Head 1 is—

(a) a disclosure authorised by the warrant;

(b) a disclosure authorised by the person to whom the warrant is or was addressed or under any arrangements made by that person for the purposes of this section;

(c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the warrant.

(3) Head 2 is—

(a) a disclosure made to, or authorised by, a Judge;

(b) a disclosure made to the Director of Public Prosecutions;

(c) a disclosure made to the Commissioner of Police for the purposes of making a complaint in connection with the execution of a warrant.

(4) Head 3 is—

(a) a disclosure made by an attorney-at-law—

(i) in contemplation of, or in connection with, any legal proceedings; and

(ii) for the purposes of those proceedings;

(b) a disclosure made—

(i) by an attorney-at-law ("A") to A's client or a representative of A's client; or

(ii) by A's client, or by a representative of A's client, to A,

in connection with the giving, by A to A's client, of advice about the effect of the relevant provisions.

(5) Head 4 is a disclosure, including a disclosure of information, that does not relate to any particular warrant but relates to warrants in general.

(6) A disclosure within Head 3 is not an excepted disclosure if it is made with the intention of furthering a criminal purpose.

(7) In subsection (4)*(b)* "the relevant provisions" means the provisions of this Part.

Offence of making unauthorised disclosures

48. (1) A person who knowingly fails to comply with section 46(1) commits an offence.

(2) A person who commits an offence under this section is liable on summary conviction to a fine of $40,000 or to a term of imprisonment of two years, or to both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

PART IV

PROTECTED INFORMATION

Application for a disclosure order

49. (1) This section applies where any protected information—

(a) has come into the possession of an authorised officer by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of an authorised officer by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications, or is likely to do so;

(c) has come into the possession of an authorised officer by means of the exercise of any power conferred by an authorisation under section 56 or 58, or as a result of the giving of a notice in pursuance of an authorisation under section 56 or 58, or is likely to do so;

(d) has come into the possession of an authorised officer as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) or has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the police, or is likely so to come into the possession of the police.

(2) The Director of Public Prosecutions may, on behalf of the authorised officer apply, *ex parte*, to a Judge in Chambers for a disclosure order.

(3) An application referred to in subsection (2) shall be in writing and shall be accompanied by an affidavit deposing the following—

(a) the name of the authorised officer on behalf of whom the application is made;

(b) full particulars of all the facts or allegations giving rise to the application;

(c) the ground, or grounds, referred to in section 50(1), on which the application is made;

(d) the basis for believing that a key to the protected information is in the possession of—

(i) a specified person; or

(ii) more than one person;

(e) details of any other investigative procedures which have been applied and failed to obtain possession of the protected information in an intelligible form.

(4) Where subsection (3)*(d)*(i) applies, the application shall contain the name and any other identifying details of the person concerned.

(5) Where subsection (3)*(d)*(ii) applies, the application shall contain the name and any other identifying details of all persons concerned, including those of any person believed to be in possession of the key—

(a) in his capacity as an officer or employee of any body corporate;

(b) as the body corporate itself or another officer or employee of the body corporate;

(c) in his capacity as an officer or employee of a firm;

(d) as the firm itself or a partner of the firm.

(6) In subsection (1)*(b)* the reference to obtaining secondary data from communications is to be read in accordance with section 11.

Issuance of a disclosure order

50. (1) A Judge may make a disclosure order if satisfied that—

(a) a key to the protected material is in the possession of any person;

(b) the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (2); or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty;

(c) the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition; and

(d) it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section.

(2) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the Islands.

(3) A disclosure order made under subsection (1) imposing a disclosure requirement in respect of any protected information—

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) must describe the protected information to which the order relates;

(c) must specify the matters falling within subsection (1)*(b)*(i) or (ii) by reference to which the notice is given;

(d) must specify the time by which the notice is to be complied with; and

(e) must set out the disclosure that is required by the notice and the form and manner in which it is to be made,

and the time specified for the purposes of paragraph *(d)* must allow a period for compliance which is reasonable in all the circumstances.

(4) A Judge shall not make an order under subsection (1) directing that the order can be complied with only by the disclosure of a key to the information unless he believes—

(a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and

(b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself.

(5) The matters to be taken into account in considering whether the requirement of subsection (4*)(b)* is satisfied in the case of any direction shall include—

(a) the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key; and

(b) any adverse effect that the giving of the direction might have on a business carried on by the person on whom the disclosure requirement is imposed.

(6) Where it appears to a person with the appropriate permission—

(a) that more than one person is in possession of the key to any protected information;

(b) that any of those persons is in possession of that key in his capacity as an officer or employee of any body corporate; and

(c) that another of those persons is the body corporate itself or another officer or employee of the body corporate,

an order under this section shall not be given, by reference to his possession of the key, to any officer or employee of the body corporate unless he is a senior officer of the body corporate or it appears to the Judge that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice.

(7) Where it appears to a person with the appropriate permission—

(a) that more than one person is in possession of the key to any protected information;

(b) that any of those persons is in possession of that key in his capacity as an employee of a firm; and

(c) that another of those persons is the firm itself or a partner of the firm,

an order under this section shall not be given, by reference to his possession of the key, to any employee of the firm unless it appears to the Judge that there is neither a partner of the firm nor a more senior employee of the firm to whom it is reasonably practicable to give the notice.

(8) Subsections (6) and (7) shall not apply to the extent that there are special circumstances of the case that mean that the purposes for which the order is given would be defeated, in whole or in part, if the order were given to the person to whom it would otherwise be required to be given by those subsections.

(9) An order under this section shall not require the making of any disclosure to any person other than the person specified in or otherwise identified by, or in accordance with, the provisions of the order.

(10) An order under this section shall not require the disclosure of any key which—

(a) is intended to be used for the purpose only of generating electronic signatures; and

(b) has not in fact been used for any other purpose.

Effect of a disclosure order

51. (1) Subject to the following provisions of this section, the effect of a disclosure order issued under section 50, imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—

(a) shall be entitled to use any key in his possession to obtain access to the information or to put it in an intelligible form; and

(b) shall be required, in accordance with the disclosure order, to make a disclosure of the information in an intelligible form.

(2) A person subject to a requirement under subsection (1)*(b)* to make a disclosure of any information in an intelligible form shall be taken to have complied with that requirement if—

(a) he makes, instead, a disclosure of any key to the protected information that is in his possession; or

(b) that disclosure is made, in accordance with the disclosure order, to the person to whom, and by the time by which, he was required to provide the information in that form.

(3) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a disclosure order—

(a) that person is not in possession of the information;

(b) that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form; or

(c) the order states, in pursuance of a direction referred to in section 50(4), that it can be complied with only by the disclosure of a key to the information,

the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to make a disclosure of any key to the protected information that is in his possession at a relevant time.

(4) Subsections (5) to (7) apply where a person ("the person given notice")—

(a) is entitled or obliged to disclose a key to protected information for the purpose of complying with any disclosure requirement imposed by a disclosure order; and

(b) is in possession of more than one key to that information.

(5) It shall not be necessary, for the purpose of complying with the requirement, for the person ordered to make a disclosure of any keys in addition to those the disclosure of which is, alone, sufficient to enable the person to whom they are disclosed to obtain access to the information and to put it into an intelligible form.

(6) Where—

(a) subsection (5) allows the person ordered to comply with a requirement without disclosing all of the keys in his possession; and

(b) there are different keys, or combinations of keys, in the possession of that person the disclosure of which would, under that subsection, constitute compliance,

the person given notice may select which of the keys, or combination of keys, to disclose for the purpose of complying with that requirement in accordance with that subsection.

(7) Subject to subsections (5) and (6), the person given the disclosure order shall not be taken to have complied with the disclosure requirement by the disclosure of a key unless he has disclosed every key to the protected information that is in his possession at a relevant time.

(8) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a disclosure order—

(a) that person has been in possession of the key to that information but is no longer in possession of it;

(b) if he had continued to have the key in his possession, he would have been required by virtue of the order to disclose it; and

(c) he is in possession, at a relevant time, of information to which subsection (9) applies,

the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the order imposing the requirement, to disclose all such information to which subsection (9) applies as is in his possession and as he may be required, in accordance with that order, to disclose by the person to whom he would have been required to disclose the key.

(9) This subsection applies to any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form.

(10) In this section "relevant time", in relation to a disclosure requirement imposed by a disclosure order, means the time of the giving of the order or any subsequent time before the time by which the requirement falls to be complied with.

Failing to comply with a disclosure order

52. (1) A person upon whom a disclosure order has been served commits an offence if he knowingly fails, in accordance with the order, to make the disclosure required by that order.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the service of that order, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the service of the order and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if—

(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and

(b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show—

(a) that it was not reasonably practicable for him to make the disclosure required by the disclosure

order before the time by which he was required, in accordance with that notice, to make it; and

(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

(5) A person who commits an offence under this section shall be liable to a fine of $20,000 or to a term of imprisonment for one year, or to both.

Tipping off

53. (1) This section applies where a disclosure order contains a provision requiring—

(a) the person to whom the disclosure order is served; and

(b) every other person who becomes aware of it or of its contents,

to keep secret the making of the order, its contents and things done pursuant to it.

(2) A disclosure order shall not contain a requirement to keep anything secret except where the protected information to which it relates has come, or is likely to come, into possession of an authorised officer by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of safety or well-being of any person, to keep secret from a particular person.

(3) A person who makes a disclosure to any other person of anything that he is required by a disclosure order to keep secret commits an offence and is liable on summary conviction to a fine of $20,000 or to term of imprisonment of one year, or to both.

(4) In proceedings against a person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that—

(a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and

(b) the person could not reasonably have been expected to take steps, after the disclosure order was served upon him or, as the case may be, becoming aware of it or its contents, to prevent the disclosure.

(5) In proceedings against a person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that—

(a) the disclosure was made by or to an attorney-at-law in connection with the giving, by the attorney-at-law to any client of his, of advice about the effect of provisions of this Part; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(6) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was made by an attorney-at-law—

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(7) Neither subsection (5) nor subsection (6) applies in the case of a disclosure made with a view to furthering any criminal purpose.

(8) In proceedings against any person for an offence under this section, it shall be a defence for that person to show that the disclosure was made to a Judge or authorised—

(a) by the Judge;

(b) by the terms of a disclosure order; or

(c) by or on behalf of a person who—

(i) is in lawful possession of the protected information to which the disclosure order relates; and

(ii) came into possession of the information as mentioned in section 50(1).

(9) In proceedings for an offence under this section against a person other than the person to whom the disclosure order was served, it shall be a defence for the person against whom the proceedings are brought to show that he neither knew nor had reasonable grounds for suspecting that the order contained a requirement to keep secret what was disclosed.

General duties of authorised officer

54. (1) An authorised officer who obtains a disclosure order shall ensure that such arrangements are in force as are necessary for securing—

(a) that a key disclosed in pursuance of the disclosure order is used for obtaining access to, or putting into

an intelligible form, only protected information in relation to which the order was given;

(b) that the uses to which a key so disclosed is put are reasonable having regard both to the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case;

(c) that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use or retention;

(d) that the requirements of subsection (2) are satisfied in relation to any key disclosed in pursuance of the disclosure order;

(e) that, for the purpose of ensuring that those requirements are satisfied, any key so disclosed is stored, for so long as it is retained, in a secure manner;

(f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form.

(2) The requirements of this subsection are satisfied in relation to any key disclosed in pursuance of a disclosure order if—

(a) the number of persons to whom the key is disclosed or otherwise made available; and

(b) the number of copies made of the key,

are each limited to the minimum that is necessary for the purpose of enabling protected information to be put into an intelligible form.

(3) Subject to subsection (4), where any relevant person incurs any loss or damage as a consequence of—

(a) any breach by a person of the duty imposed upon them by subsection (1); or

(b) any contravention by any person whatever of arrangements made in pursuance of subsection (1) in relation to persons under the control of a person to whom this section applies,

the breach or contravention shall be actionable against the person to whom this section applies at the suit or instance of the relevant person.

(4) A person is a relevant person for the purposes of subsection (3) if he is—

(a) a person who has made a disclosure in pursuance of a disclosure order; or

(b) a person whose protected information or key has been disclosed in pursuance of such a disclosure order,

and loss or damage shall be taken into account for the purposes of subsection (3) to the extent only that it relates to the disclosure of a particular protected information or a particular key which, in the case of a person falling within paragraph *(b)*, shall be his information or key.

(5) For the purposes of subsection (4)—

(a) information belongs to a person if he has any right that would be infringed by an unauthorised disclosure of the information; and

(b) a key belongs to a person if it is a key to information that belongs to him or he has any right that would be infringed by an unauthorised disclosure of the key.

Interpretation of Part IV

55. (1) References in this Part to a person's 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 otherwise supplied to him; and

(c) to its being, or being contained in, anything which he or 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.

(2) References in this Part to something's being intelligible or being put into an intelligible form include references to its being in the condition in which it was before an encryption or similar process was applied to it or, as the case may be, to its being restored to that condition.

(3) In the definition of "electronic signature" in section 2—

(a) references to the authenticity of any communication or data are references to any one or more of the following—

(i) whether the communication or data comes from a particular person or other source;

(ii) whether it is accurately timed and dated;

(iii) whether it is intended to have legal effect; and

(b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

PART V

COMMUNICATIONS DATA

Power to grant authorisations

56. (1) Subsection (2) applies if the Governor, on an application made by an authorised officer, considers—

(a) that it is necessary for the authorised officer to obtain communications data for a purpose falling within subsection (7);

(b) that it is necessary for the authorised officer to obtain the data for the purposes of a specific investigation or a specific operation; and

(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The Governor may authorise the authorised officer to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person; and

(b) relates to—

(i) a telecommunication system; or

(ii) data derived from a telecommunication system.

(3) Subsections (1) and (2) are subject to sections 58 and 62.

(4) Authorised conduct may, in particular, consist of an authorised officer—

(a) obtaining the communications data himself from any person or telecommunication system;

(b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it); and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation; or

(c) requiring by notice endorsed by or on behalf of the Governor a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it); and

(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation;

(b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned; and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) in the interests of national security;

(b) for the applicable crime purpose;

(c) in the interests of the economic well-being of the Islands so far as those interests are also relevant to the interests of national security;

(d) in the interests of public safety;

(e) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;

(f) to assist investigations into alleged miscarriages of justice;

(g) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P; or

(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

(8) In subsection (7)*(b)*, "the applicable crime purpose" means—

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting any offences specified in the Schedule;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

Power of designated senior officer to grant authorisations: urgent cases

57. (1) Subsection (2) applies if a designated senior officer considers—

(a) that it is necessary for an authorised officer to obtain communications data for a purpose falling within subsection (7);

(b) that it is necessary for an authorised officer to obtain the data for the purposes of a specific investigation or a specific operation;

(c) that there is an urgent need to obtain the data; and

(d) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The designated senior officer may authorise any police officer to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person; and

(b) relates to—

(i) a telecommunication system; or

(ii) data derived from a telecommunication system.

(3) Subsections (1) and (2) are subject to sections 58 and 62.

(4) Authorised conduct may, in particular, consist of an authorised police officer—

(a) obtaining the communications data himself from any person or telecommunication system;

(b) asking any person whom the authorised police officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it); and

(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation; or

(c) requiring by notice endorsed by or on behalf of the designated senior officer a telecommunications operator whom the authorised police officer believes is, or may be, in possession of the communications data or capable of obtaining it—

(i) to obtain the data (if not already in possession of it); and

(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—

(a) may relate to data whether or not in existence at the time of the authorisation;

(b) may authorise the obtaining or disclosure of data by a person who is not an authorised police officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned; and

(c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation—

(a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system; and

(b) may not authorise an authorised police officer to ask or require, in the circumstances mentioned in subsection (4)*(b)* or *(c)*, a person to disclose the data to any person other than a police officer.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—

(a) for the applicable crime purpose;

(b) in the interests of public safety;

(c) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;

(d) to assist investigations into alleged miscarriages of justice;

(e) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P; or

(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

(8) In subsection (7)*(a)*, "the applicable crime purpose" means—

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting any offences specified in the Schedule;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

(9) For the purposes of this section, "authorised police officer" means a police officer authorised by a designated senior officer under subsection (2).

Restrictions in relation to internet connection records

58. (1) The Governor may not, on the application of an authorised officer, grant an authorisation under section 56 for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.

(2) A designated senior officer may not grant an authorisation under section 57 for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.

(3) Condition A is that [the person with power to grant the authorisation] considers that it is necessary, for a purpose falling within section 56(7) or 57(7) (as applicable) to obtain the data to identify which person or apparatus is using an internet service where—

(a) the service and time of use are already known; but

(b) the identity of the person or apparatus using the service is not known.

(4) Condition B is that—

(a) the purpose for which the data is to be obtained falls within section 56(7) or 57(7) (as applicable) but is not the purpose of preventing or detecting serious crime mentioned in section 56(8)*(a)* or 57(8)*(a)* or the purpose of preventing or detecting crime mentioned in section 56(8)*(b)* or 57(8)*(b)*; and

(b) the [the person with power to grant the authorisation] considers that it is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known;

(ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime; or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) Condition C is that—

(a) either—

(i) the purpose for which the data is to be obtained is the purpose of preventing or detecting serious crime mentioned in section 56(8)*(a)* or 57(8)*(a)*; or

(ii) the purpose for which the data is to be obtained is the purpose of preventing or detecting crime mentioned in section 56(8)*(b)* or 57(8)*(b)*, and the crime to be prevented or detected is serious crime; and

(b) the person with power to grant the authorisation considers that is necessary to obtain the data to identify—

(i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known;

(ii) the where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime; or

(iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

Procedure for authorisations and authorised notices

59. (1) An authorisation shall specify—

(a) whether the authorisation has been granted by the Governor under section 56 or by a designated senior officer under section 57;

(b) the matters falling within section 56(7) or 57(7) (as applicable) by reference to which it is granted;

(c) the conduct that is authorised;

(d) the data or description of data to be obtained; and

(e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.

(2) An authorisation granted by a designated senior officer under section 57 shall also specify the office, rank or position held by the officer.

(3) An authorisation which authorises a person to impose requirements by notice on a telecommunications operator shall also specify—

(a) the operator concerned; and

(b) the nature of the requirements that are to be imposed,

but need not specify the other contents of the notice.

(4) The notice itself—

(a) must specify—

(i) the office, rank or position held by the person giving it;

(ii) the requirements that are being imposed; and

(iii) the telecommunications operator on whom the requirements are being imposed; and

(b) must be given in writing and endorsed by or on behalf of the Governor or the designated senior officer (as applicable).

(5) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

Duration and cancellation of authorisations and notices

60. (1) An authorisation under section 56 ceases to have effect at the end of the period of one month beginning with the date on which it is granted.

(2) An authorisation may be renewed at any time before the end of that period by the grant of a further authorisation.

(3) Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.

(4) An authorisation under section 57 ceases to have effect at the end of the period of three days beginning with the date on which it is granted.

(5) Where the Governor has granted an authorisation under section 56—

(a) the Governor may cancel it at any time; and

(b) the Governor shall cancel it if the Governor considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.

(6) Where a designated senior officer has granted an authorisation under section 57—

(a) the designated senior officer may cancel it at any time; and

(b) the designated senior officer shall cancel it if the designated senior officer considers that the requirements of this Part would not be satisfied in relation to granting an equivalent new authorisation.

(7) A notice given in pursuance of an authorisation (and any requirement imposed by the notice)—

(a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1) or (4); but

(b) is cancelled if the authorisation is cancelled under subsection (5) or (6).

Duties of telecommunications operators in relation to authorisations

61. (1) It is the duty of a telecommunications operator on whom a requirement is imposed by notice given in pursuance of an authorisation to comply with that requirement.

(2) It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or requirement for the data in pursuance of an authorisation, to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned.

(3) A person who is under a duty by virtue of subsection (1) or (2) is not required to take any steps in pursuance of that duty which it is not reasonably practicable for that person to take.

(4) The duty imposed by subsection (1) or (2) is enforceable by civil proceedings by the Attorney General for an injunction, or for any other appropriate relief.

Judge approval for authorisations to identify or confirm journalistic sources

62. (1) Subsection (2) applies if—

(a) the Governor has granted an authorisation under section 56 or a designated senior officer has granted an authorisation under section 57 in relation to the obtaining by an authorised officer of communications data for the purpose of identifying or confirming a source of journalistic information; and

(b) the authorisation is not necessary because of an imminent threat to life.

(2) The authorisation is not to take effect until such time (if any) as a Judge has approved it.

(3) The Director of Public Prosecutions, on behalf of the authorised officer, may apply to a Judge for approval of the authorisation.

(4) The applicant is not required to give notice of the application to—

(a) any person to whom the authorisation relates; or

(b) that person's legal representatives.

(5) A Judge may approve the authorisation if, and only if, the Judge considers that—

(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation; and

(b) at the time when the Judge is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) In considering whether the position is as mentioned in subsection (5)*(a)* and *(b)*, the Judge must, in particular, have regard to—

(a) the public interest in protecting a source of journalistic information; and

(b) the need for there to be another overriding public interest before the authorised officer seeks to identify or confirm a source of journalistic information.

(7) Where, on an application under this section, the Judge refuses to approve the grant of the authorisation, the Judge may quash the authorisation.

Lawfulness of conduct authorised by this Part

63. Conduct is lawful for all purposes if—

(a) it is conduct in which any person is authorised to engage by an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation, and

(b) the conduct is in accordance with, or in pursuance of, the authorisation or notice.

Offence of making unauthorised disclosure

64. (1) It is an offence for a telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of—

(a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person; or

(b) any request made in pursuance of an authorisation for the operator to disclose such data.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the authorised officer who is seeking to obtain the data from the operator (whether the permission is contained in any notice requiring the operator to disclose the data or otherwise).

(3) A person who commits an offence under this section is liable on summary conviction to a fine of $40,000 or to a term of imprisonment of five years, or to both.

Admissibility of communications data

65. (1) Subject to subsection (2), communications data obtained in accordance with section 56 or 57 shall be admissible in evidence in accordance with the law relating to the admissibility of evidence.

(2) In admitting into evidence any communications data referred to in subsection (1)—

(a) no question shall be asked of any witness that discloses or might result in the disclosure of any of the details pertaining to the method by which the data was obtained or the identity of any party who supplied the data;

(b) a statement by the witness that the data was obtained by virtue of an authorisation to obtain communications data shall be sufficient disclosure as to the source or origin of the data; and

(c) in proving the truth of a statement referred to in paragraph *(b)*, the witness shall not be asked to disclose any of the matters referred to in paragraph *(a)*.

(3) Subsection (2) shall not apply to any proceedings in respect of an offence under this Ordinance, but if the court is satisfied that—

(a) the disclosure would be likely to jeopardise the course of any investigation or be prejudicial to the interests of internal security; and

(b) the parties to the proceedings would not be unduly prejudiced thereby,

the court shall not require or permit disclosure of the matters referred to in subsection(2)*(a)*.

PART VI

INTERCEPTION EQUIPMENT

Listed equipment

66. (1) The Governor may, by order published in the *Gazette*, declare any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for the purposes of interception of communications, subject to such conditions or circumstances specified in the notice, to be listed equipment with interception capabilities.

(2) An order under subsection (2) may at any time in like manner be amended or withdrawn.

(3) The first order to be issued by the Governor under subsection (1) shall be published in the *Gazette* within three months after the date of commencement of this Ordinance, or as soon as reasonably practicable thereafter.

(4) Subject to subsection (5), before the Governor exercises the powers conferred upon him under subsection (1), he shall cause to be published in the *Gazette* a draft of the proposed order, together with a notice inviting all interested parties to submit to him in writing and within a specified period, comments and representations in connection with the proposed order.

(5) A period not exceeding one month shall elapse between the publication of the draft order and the publication of the order under subsection (1).

(6) Subsection (4) does not apply—

(a) if the Governor, after consideration of comments and representations received in terms of subsection (4) decides to publish an order referred to in subsection (1) in an amended form; or

(b) to any declaration in terms of subsection (1) in respect of which the Governor is of the opinion that the public interest requires that it be made without delay.

(7) An order under subsection (1) shall, before publication in the *Gazette*, be laid before the House of Assembly and shall be subject to affirmative resolution.

Prohibition on manufacture and possession of listed equipment

67. (1) Subject to subsection (2) and section 68, a person shall not manufacture, assemble, possess, sell, or purchase any listed equipment.

(2) Subsection (1) shall not apply to any authorised officer or any other person who manufactures, assembles, possesses, sells, purchases, or advertises listed equipment under the authority of a certificate of exemption issued to him by the Governor under section 68.

Exemptions

68. (1) The Governor may, upon application made to him, in writing, exempt a person from one or all of the prohibited acts listed under section 67(1) for such period and on such terms as the Governor may determine.

(2) The Governor shall not grant an exemption under subsection (1) unless he is satisfied that—

(a) the exemption is in the public interest; or

(b) special circumstances exist which justify the exemption.

(3) An exemption under subsection (1) shall be granted by issuing to the person concerned a certificate of exemption in which his name, and the scope, period and conditions of the exemption are specified.

(4) A certificate of exemption granted under subsection (3) shall be published in the *Gazette* and shall become valid upon the date of such publication.

(5) A certificate of exemption may at any time in like manner be amended or withdrawn by the Governor.

(6) A certificate of exemption lapses upon—

(a) termination of the period for which it was granted; or

(b) withdrawal under subsection (5).

Offence for contravention of section 67

69. (1) A person who contravenes or fails to comply with section 67 commits an offence and shall be liable on conviction to a fine of $50,000 or a term of imprisonment for five years, or to both.

(2) A court convicting a person of an offence under subsection (1) shall in addition to any penalty which it may impose in respect of the offence, declare any listed equipment—

(a) by means of which the offence was committed;

(b) which was used in the connection with the commission of the offence;

(c) which was found in the possession of the convicted person; or

(d) the possession of which constituted the offence,

to be forfeited and disposed of in accordance with section 70.

(3) Any listed equipment declared forfeited under subsection (2) shall, as soon as practicable after the date of declaration of forfeiture be delivered to the Commissioner of Police.

Disposal of forfeited listed equipment

70. (1) A declaration of forfeiture made pursuant to section 69(2) shall not affect any right which a person has to the listed equipment, if the person can show that the relevant criteria are met.

(2) For the purposes of subsections (1) and (4), the relevant criteria are—

(a) the person is not the person convicted of an offence under section 69(1) which resulted in the listed equipment being forfeited under section 69(2);

(b) at the time of the commission of the offence referred to in subsection (1) he was lawfully in possession of an exemption issued under section 68;

(c) the exemption related to the listed equipment referred to in subsection (1);

(d) he took all reasonable steps to prevent the use of the listed equipment in connection with the offence referred to in subsection (1); and

(e) he could not reasonably have known or had no reason to suspect that the listed equipment concerned was being or would be used in connection with that offence.

(3) An application may be made to a Judge at any time within a period of three months with effect from the date of declaration of forfeiture under section 69(2), by any person claiming a right to the forfeited listed equipment.

(4) If the Judge is satisfied on hearing an application made under subsection (3) that the applicant has met the relevant criteria, the Judge shall set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to the person.

(5) Where, in relation to listed equipment which is subject to a declaration of forfeiture—

(a) an application has not been made in accordance with subsection (3); or

(b) a Judge has determined an application pursuant to subsection (4) and did not set aside the declaration of forfeiture; and

(c) at least four months have elapsed from the date of forfeiture under section 69(2),

the Commissioner of Police shall, as soon as practicable, destroy the listed equipment which are subject of that declaration of forfeiture.

PART VII

MISCELLANEOUS

Payments towards certain compliance costs

71. (1) The Governor may put in place arrangements for enabling telecommunications operators and postal operators to receive an appropriate contribution in respect of such of their relevant costs as the Governor considers appropriate.

(2) Any arrangements may provide for payment of a contribution to be subject to terms and conditions determined by the Governor.

(3) Such terms and conditions may, in particular, include a condition on the operator concerned to comply with any audit that may reasonably be required to monitor the claim for costs.

(4) Any arrangements may provide for the Governor to determine—

(a) the scope and extent of the arrangements; and

(b) the appropriate level of contribution which should be made in each case.

(5) Different levels of contribution may apply for different cases or descriptions of case.

(6) For the purposes of complying with this section the Governor may make, or arrange for the making of, payments of money from the Consolidated Fund.

(7) In subsection (1) "relevant costs" means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with the Ordinance.

Protection of authorised officer and others

72. (1) No civil suit or criminal process shall be brought against—

(a) any senior designated officer;

(b) any authorised officer; or

(c) any person acting on the direction of a senior designated officer or an authorised officer,

in respect of any act performed by him, in good faith and with reasonable cause, in the exercise or purported exercise of his functions under this Ordinance or any regulations made under section 76.

(2) A person (whether or not the person so authorised or required) is not to be subject to any civil liability in respect of conduct that—

(a) is incidental to, or is reasonably undertaken in connection with, conduct that is lawful by virtue of section 63; and

(b) is not itself conduct for which an authorisation or warrant—

(i) is capable of being granted under this Ordinance; and

(ii) might reasonably have been expected to have been sought in the case in question.

False statements

73. A person who, in any application made under, or as required by, this Ordinance, makes a statement which he knows to be false in any material particular commits an offence and is liable on summary conviction to a fine of $40,000 or to a term of imprisonment for two years, or to both.

Offences by body corporate

74. Where an offence under this Ordinance is committed by a body corporate and it is proved that the offence has been committed with the consent or connivance of, or is attributable to neglect by, a director, manager, secretary or other officer of the body corporate or a person purporting to act in such capacity, the officer or person as well as the body corporate shall be liable to be proceeded against and punished accordingly.

Annual report

75. (1) The Commissioner of Police shall, within three months, after the end of each year, in relation to the operation of this Ordinance in the immediately preceding year, prepare a report relating to—

(a) the number of warrants applied for to intercept communications;

(b) the number of warrants granted by the Court;

(c) the number of warrants applied for and granted under section 15;

(d) the average period for which warrants were given;

(e) the number of warrants refused or revoked by the Court;

(f) the number of applications made for renewals;

(g) the number and nature of interceptions made pursuant to the warrants granted;

(h) the offences in respect of which warrants were granted, specifying the number of warrants given in respect of each of those offences;

(i) the numbers of persons arrested whose identity became known to an authorised officer as a result of an interception under a warrant;

(j) the number of criminal proceedings commenced by the Crown in which private communications obtained by interception under a warrant were adduced in evidence and the number of those proceedings that resulted in a conviction;

(k) the number of criminal investigations in which information obtained as a result of the interception of a private communication under a warrant was used although the private communication was not adduced in evidence in criminal proceedings commenced by the Crown as a result of the investigations;

(l) the number of prosecutions commenced against persons under sections 7, 8, 38, 43, 48. 52, 53, 64, 69 and 73 and the outcome of those prosecutions;

(m) a general assessment of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences in the Islands; and

(n) any other matter he considers necessary.

(2) The Commissioner of Police shall cause a copy of the report prepared by him under subsection (1) to be laid before the House of Assembly within one month after its completion.

Amendment of Schedule

76. (1) The Governor may, by order, amend the Schedule.

(2) An order made under subsection (1) shall be subject to affirmative resolution of the House of Assembly.

Regulations

77. The Governor may make Regulations prescribing any matter or thing in respect of which it may be expedient to make regulations for the purpose of carrying this Ordinance into effect.

Consequential amendment

78. Section 15 of the Telecommunications Ordinance is amended by repealing subsection (4) and substituting the following—

"(4) Subsection (2) shall not apply to a licensee to the extent necessary to comply with the terms of a warrant issued under Chapter 1 or 2 of Part III of the Interception of Communications Ordinance.".

SCHEDULE

APPLICABLE OFFENCES

(Sections 2(4), 14(2)(b), 24(2)(b), 56(8)(a) and 57(8)(a))

1. Murder or treason
2. Kidnapping or abduction
3. Rape
4. Sexual exploitation of children
5. Money laundering offence contrary to the Proceeds of Crime Ordinance
6. An offence contrary to the Prevention of Terrorism Ordinance
7. Trafficking in persons contrary to the Trafficking in Persons (Prevention) Ordinance
8. Assisting illegal entry contrary to the Immigration Ordinance
9. Producing, manufacture, supplying or otherwise dealing in any controlled drug in contravention of the Control of Drugs Ordinance
10. Importing or exporting a controlled drug specified in Parts I, II or III of the First Schedule of the Control of Drugs Ordinance in contravention of that Ordinance
11. Importation or exportation of firearm in contravention of the Customs Ordinance
12. An offence contrary to the Anti-Gang Ordinance
13. An offence contrary to the to the Firearms Ordinance
14. An offence contrary to the Integrity Commission Ordinance
15. An offence contrary to the applicable International Convention on hijacking, terrorist offences or people trafficking
16. Attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs.