INTERCEPTION OF COMMUNICATIONS ACT, 2010

ARRANGEMENT OF SECTIONS

PART I PRELIMINARY

- 1. Short title
- 2. Interpretation

PART II INTERCEPTION OF COMMUNICATIONS

- 3. Prohibition of interception
- 4. Other interception related offences
- 5. Application for interception direction, etc.
- 6. Issuance of interception direction
- 7. Scope and form of interception direction
- 8. Duration and renewal of interception direction
- 9. Condition for issuance of entry warrant, etc.
- 10. Termination of interception direction, etc.
- 11. Modification of interception direction and entry warrant
- 12. Reports on progress

PART III PROTECTED INFORMATION AND TRAFFIC DATA

- 13. Unauthorised interception of protected information, etc.
- 14. Order requiring disclosure of protected information, etc.
- 15. Effects of disclosure order

PART IV EXECUTION OF INTERCEPTION DIRECTIONS, ENTRY WARRANTS, ETC.

- 16. Execution of interception direction, etc.
- 17. Entry on premises for execution of warrant
- 18. Duty to provide assistance
- 19. Penalty for unauthorised disclosure of communication, etc.
- 20. Admissibility of intercepted or disclosed communication, etc.
- 21. Exclusion of matters from legal proceedings
- 22. Exceptions to section 21

PART V LISTED EQUIPMENT

- 23. Council as sole authority on equipment
- 24. Prohibition on possession of listed equipment
- 25. Exemptions
- 26. Penalty for contravention of section 24

PART VI MISCELLANEOUS

- 27. False statements
- 28. Amendment of Schedule
- 29. Regulations
- 30. Code of conduct
- 31. Disclosure of information
- 32. Interception in prisons
- 33. Protection for acts done in good faith
- 34. Commencement

SCHEDULE



No. 25 of 2010

I assent,

(SIR COLVILLE N. YOUNG) Governor-General

16th December, 2010

AN ACT to provide for the interception of communications and the provision of information relating to interception in Belize; and to provide for matters connected therewith or incidental thereto.

(Gazetted 18th December, 2010.)

BE IT ENACTED, by and with the advice and consent of the House of Representatives and the Senate of Belize and by the authority of same, as follows:

PART I PRELIMINARY

1. This Act may be cited as the

Short title.

INTERCEPTION OF COMMUNICATIONS ACT, 2010.

Interpretation.

2. (1) In this Act, unless the context otherwise requires:

"attorney-at-law" has the meaning given to it under section 2 of the *Legal Profession Act*;

CAP. 320.

"authorised officer" means the Commissioner of Police; or

- (a) a person for the time being lawfully exercising the functions of the Commissioner of Police;
- (b) an officer authorised in writing to act on behalf of the Commissioner of Police; or
- (c) the Chief Executive Officer in the Ministry responsible for the Belize Police Department;
- (d) any person employed by or assigned to any law enforcement agency under the Government who is explicitly authorised by the Commissioner of Police to carry out lawful interception and related functions under this Act.

CAP. 138.

"Commissioner" means the Commissioner of Police appointed under section 3 of the *Police Act*;

"communication" includes:

- (a) except in the definition of "postal service", anything encrypted or unencrypted transmitted by means of a postal service including a postal article;
- (b) anything encrypted or unencrypted comprising speech, music, sounds, visual images or data of any description; and
- (c) encrypted or unencrypted 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;

"communication data" means any:

- (a) encrypted or unencrypted data comprised in or attached to a communication, whether by the sender or otherwise, for the purposes of any postal service or communication network by means of which the communication is being or may be transmitted;
- (b) encrypted or unencrypted information, that does not include the contents of a communication, other than data falling within paragraph (a) which is about the use, made by any person:
 - (i) of any postal service or communication network; or
 - (ii) of any part of a communication network in connection with the provision to or use by any person of any communication service; and
- (c) encrypted or unencrypted information not falling within paragraph (a) or paragraph (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal or a communication service;

"communication provider" means a person who operates a communication network or who provides a communication service including, but not limited to, radio, telecommunications, and internet service providers;

"communication network" means any wire, radio, optical or other electromagnetic system used to route switch or transmit communication;

"communication service" means a service that consists in the provision of access to and of facilities for making use of, any communication network, whether or not it is one provided by the person providing the service; CAP. 4.

"Council" means the National Security Council;

"Director of Public Prosecutions" means the Director of Public Prosecutions appointed under section 108 of the Belize Constitution;

"disclosure order" means an order made pursuant to section 14, requiring access to electronic data;

"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, and the establishment of its integrity or both;

"encrypt" means the use of codes, ciphers, mechanical systems, or electronic algorithms so as to make visual images, speech, music, sounds, or data of any description, which would otherwise be intelligible, unintelligible from its intended meaning and requiring corresponding codes, ciphers, mechanical systems, or electronic algorithms to become, once again, intelligible;

"intercept" includes:

(a) aural or other acquisition of the contents of a communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication;

- (b) monitoring a communication by means of a monitoring device;
- (c) viewing, examining, or inspecting the contents of a communication;
- (d) diverting of any communication from its intended destination to any other destination; and
- (e) cloning of telecommunication equipment by configuring or otherwise modifying telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorisation.

and "interception" shall be construed accordingly;

"intercepted communication" means a communication which during the course of its transmission by means of a postal service or a communication network is intercepted;

"interception device" means any electronic, mechanical or other instrument, device, equipment or apparatus, or software 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 a customer by a communication provider in the ordinary course of business

- and being used by the customer in the ordinary course of his business;
- (b) furnished by a customer for connection to the facilities of a communication service and being used by the customer in the ordinary course of business; or
- (c) being used by a communication provider in the ordinary course of business;

"interception direction" means an interception direction issued pursuant to section 6;

"Judge" means a Judge of the Supreme Court;

"key" in relation to electronic data, means a 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 electronic data into an intelligible form;

"listed equipment" means:

- (a) any equipment declared to be listed equipment pursuant to section 23; or
- (b) a component of equipment referred to in paragraph (a);
- "Minister" means the Minister responsible for the Police;
- "Police Department" means the Belize Police Department established under section 4 of the *Police Act*;

"postal article" means:

- (a) any form of written communication, or any other document or article:
 - (i) that is addressed to a specific person or a specific address; and
 - (ii) that is to be conveyed other than by electronic means; and
 - (iii) for which a charge is made in respect of carrying, taking charge of, sending it or delivering; or
- (b) an envelope, packet, package, or wrapper containing a communication, document or article;

"postal provider" means a person who provides a postal service;

"postal service" means a service which:

- (a) consists of the following, or any one or more of them, namely the collection, sorting, conveyance, distribution and delivery whether in Belize or elsewhere, of postal articles; and
- (b) is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to make available, or to facilitate, by means of transmission from place to place of postal articles containing communication;

[&]quot;private communication network" means a communication network that, without it being a public communication

network, is a communication network in relation to which the following conditions are satisfied:

- (a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public communication network; and
- (b) there is apparatus comprised in the communication network which is both located in Belize and used, with or without other apparatus, for making the attachment to the public communication network;

"protected information" means electronic data which, without a key, or cannot readily be accessed or put in an intelligible form;

"public postal service" means any postal service which is offered or provided to the public or to a substantial section of the public in Belize;

"public communication network" means:

- (a) a telecommunications network commonly known as a public switched telephone network including satellite, fixed, and cellular telephone services;
- (b) a communication network used by any person to provide communication services to the public including, but not limited to, radio, telecommunications, and internet service; or
- (c) a communication network whereby the public can send or receive communication service to or from:

- (i) anywhere in Belize; or
- (ii) anywhere outside Belize;

"terrorist act" has the meaning given to it under the Money CAP. 104. Laundering and Terrorism (Prevention) Act;

"traffic data" means any communication data:

- (a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication may have been, is or may be transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article;
- (b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted:
- (c) comprising signals for the actuation of:
 - (i) apparatus used for the purposes of a communication network for effecting, in whole or in part, the transmission of any communication; or
 - (ii) any communication network in which that apparatus is comprised;
- (d) identifying the data or other data as data comprised in or attached to a particular communication; or
- (e) identifying a computer file or a computer programme, access to which is obtained or which is run by means of the communication,

to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

- (2) For the purposes of this Act "the interests of national security" shall be construed as including, but not limited to, the protection of Belize from threats of sabotage, espionage, terrorist acts, terrorism, subversion or military or paramilitary invasion.
- (3) For the purpose of this Act "detection" of an offence shall be taken to include:
 - (a) establishing by whom, for what purpose, when, by what means and generally in what circumstances any offence may be committed; and
 - (b) the apprehension of the person by whom an offence was committed.

PART II INTERCEPTION OF COMMUNICATIONS

Prohibition of interception.

- 3. (1) Except as provided in this section, any person who with intent intercepts communication in the course of its transmission by means of a public postal service or a communication network without authorisation, commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;

- (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
- (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.
- (2) A person who with intent intercepts a communication in the course of its transmission by means of a public postal service or a communication network for the purpose of commercial benefit, political advantage, or criminal activity commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the first instance;
 - (b) a fine of not less than one hundred thousand dollars and not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding ten years in the second instance; and
 - (c) a fine of two hundred thousand dollars and a term of imprisonment not exceeding ten years in the subsequent instances.
- (3) A person does not commit an offence under subsection (1) if:
 - (a) the communication is intercepted in accordance with an interception direction issued pursuant to section 6 or an entry warrant issued pursuant to section 9;

- (b) that person has written or otherwise documented authorisation consenting to the interception from the person to whom or from whom the communication is transmitted;
- (c) the communication is acquired in accordance with the provisions of the Belize Telecommunications Limited Act, the Financial Intelligence Unit Act or or any other law; or
- (d) the interception is of a communication made through a communication network that is so configured as to render the communication readily accessible to the general public.
- (4) A court convicting a person of an offence under this Act may, in addition to any penalty which it imposes in respect of the offence, order the forfeiture or disposal of any device used in the commission of the offence as provided by section 26 (3) to (9).
- (5) For the purposes of this section, communication means:
 - (a) communication in the course of transmission by means of a communication network in real time; or;
 - (b) communication stored in a manner that enables the recipient to receive that communication or otherwise have access to it.

Other interception related offences.

- 4. A person who encrypts data of any description for the purpose of committing a crime or with intent utilises encrypted information for the purpose of committing a crime commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the first instance;

- (b) a fine of not less than one hundred thousand dollars and not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding ten years in the second instance; and
- (c) a fine of two hundred thousand dollars and a term of imprisonment not exceeding ten years in the subsequent instances.
- 5. (1) An authorised officer who wishes to obtain an interception direction pursuant to the provisions of this Act shall request the Director of Public Prosecutions to make an application *ex parte* to a Judge in chambers on his behalf.

Application for interception direction, etc.

- (2) An application referred to in subsection (1) shall be in the prescribed form 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) the facts or allegations giving rise to the application;
 - (c) sufficient information for a Judge to issue an interception direction;
 - (d) the ground referred to in section 6(1) on which the application is made;
 - (e) full particulars of all the facts and the circumstances alleged by the authorised officer on whose behalf the application is made including:
 - (i) if practical, a description of the nature and location of the facilities from which or the premises at which the communication is to be intercepted; and

- (ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;
- (f) if applicable, whether other investigative procedures have been applied and failed to produce the required evidence or the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;
- (g) the period for which the interception direction is required to be issued;
- (h) whether any previous application has been made for the issuing of an interception direction in respect of the same person, the same facility or the same premises specified in the application and, if such previous application exists, shall indicate the current status of that application; and
- (i) if applicable, a description of the communication equipment to be intercepted;
- (j) any other directives issued by the Judge.
- (3) Subsection (2)(d) shall not apply in respect of an application for the issuing of an interception direction on a ground referred to in section 6(1) (a) if 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 or groups classified as criminal gangs.
- (4) Where an interception direction is applied for on the grounds of national security, the application from the

authorised officer shall be accompanied by a written authorisation signed by the Minister authorising the application on that ground.

- (5) Subject to subsection (6), the records relating to an application for an interception direction 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 place as the Judge may authorise.
- (6) The records referred to in subsection (5) may be opened if a Judge so orders only:
 - (a) for the purpose of dealing with an application for further authorisation; or
 - (b) for renewal of an authorisation.
- 6. (1) An interception direction shall be issued if a Judge is satisfied, on the facts alleged in the application pursuant to section 5, that there are reasonable grounds to believe that:

Issuance of interception direction.

- (a) obtaining the information sought under the interception direction is necessary in the interests of:
 - (i) national security;
 - (ii) public order;
 - (iii) public safety; or
 - (iv) public health;

Schedule.

- (v) preventing, detecting, investigating, or prosecuting any offence specified in the Schedule, where there are reasonable grounds to believe that such an offence has been, is being or may be committed; or
- (vi) giving effect to the provisions of any mutual legal assistance agreement in circumstances appearing to the Judge to be equivalent to those in which he would issue an interception direction by virtue of sub-paragraph (v); and

(b) other procedures:

- (i) have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the interception direction;
- (ii) are too dangerous to adopt in the circumstances; or
- (iii) having regard to the urgency of the case are impracticable; and
- (c) it would be in the best interests of the administration of justice to issue the interception direction.
- (2) A Judge considering an application may require the authorised officer to furnish such further information as he deems necessary.

Scope and form of interception direction.

- 7. (1) An interception direction shall be in the prescribed form and shall permit the authorised officer to:
 - (a) intercept, at any place in Belize, any communication in the course of its transmission;

- (b) secure the interception in the course of its transmission by means of a postal service or a public or private communication network, of such communication as are described in the interception direction; and
- (c) secure the disclosure of the intercepted material obtained or required by the interception direction, and of related communication data.
- (2) An interception direction shall authorise the interception of:
 - (a) communication transmitted by means of a postal service or a public or a private communication network to or from:
 - (i) the person specified in the interception direction;
 - (ii) the premises so specified and described; or
 - (iii) the set of communication equipment so specified and described; and
 - (b) such other communication, if any as may be necessary in order to intercept communication falling within paragraph (a).
- (3) An interception direction shall specify the identity of the:
 - (a) authorised officer on whose behalf the application is made pursuant to section 5, and the person who will execute the interception direction;
 - (b) person, if known and appropriate, whose communication is to be intercepted; and

- (c) postal service provider or the communication provider to whom the interception direction to intercept must be addressed, if applicable.
- (4) An interception direction may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Act.
- (5) An interception direction issued pursuant to this section may specify conditions or restrictions relating to the interception of communications authorised therein.

Duration and renewal of interception.

- 8. (1) An interception direction shall cease to have effect at the end of the relevant period, but may be renewed at any time before the end of that period, on an application made pursuant to subsection (2).
- (2) A Judge may renew the interception direction before the expiration of the relevant period, upon an application for the renewal of an interception direction being made by the Director of Public Prosecutions on behalf of an authorised officer, if satisfied that the renewal of the interception direction is justified.
- (3) An application for the renewal of an interception direction under subsection (2) shall be in the prescribed form and shall be accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal of the interception direction.
- (4) If at any time before the end of the periods referred to in subsections (1) and (2), it appears to the authorised officer to whom the interception direction is issued, or a person acting on his behalf, that an interception direction is no longer necessary, he shall make an application to the Court for the cancellation of the interception direction and the court may cancel the interception direction.

- (5) For the purposes of this section "relevant period" means a period of up to six months as specified by the Judge beginning with the date of the issuance of the interception direction or, in the case of an interception direction that has been renewed, the date of its latest renewal.
- 9. (1) An entry warrant shall not be issued by a Judge unless there exists with respect to the premises to which the application for an entry warrant relates, a related interception direction.

Condition for issuance of entry warrant,

- (2) Where the Director of Public Prosecutions:
 - (a) makes an application for an interception direction on behalf of an authorised officer pursuant to section 5, the Director of Public Prosecutions may at the time of making the application, also apply to the Judge for the issuance of an entry warrant with respect to the premises to which the interception direction relates; or
 - (b) made an application for an interception direction on behalf of an authorised officer pursuant to section 5, the Director of Public Prosecutions may, at any such stage after the issuance of the interception direction in respect of which such an application was made, but before the expiry of the period or the extended period for which it has been issued, apply ex parte to a Judge for the issuance of an entry warrant with respect to the premises to which the interception direction relates.
- (3) Subject to section 10, an application for an entry warrant referred to in subsection (2), shall be in the prescribed form and shall:

- (a) be accompanied by an affidavit deposing the:
 - (i) name of the authorised officer on behalf of which the application is made;
 - (ii) premises in respect of which the entry warrant is required; and;
 - (iii) the specific purpose for which the application is made;
- (b) also contain, if the application is made in terms of subsection (2) (b), proof that an interception direction has been issued, and an affidavit setting forth the results, if any, obtained in the interception direction concerned from the date of its issuance up to the date on which the application was made, or a reasonable explanation of the failure to obtain such results;
- (c) indicate whether any previous application has been made for the issuing of an entry warrant for the same purpose or in respect of the same premises specified in the application and, if such previous application exists, indicate the status of the previous application; and
- (d) be accompanied by a written authorisation signed by the Minister where the application is made on the grounds of national security.
- (4) Subject to subsections (1) and (5), a Judge may upon an application made to him by the Director of Public Prosecutions on behalf of an authorised officer, issue an entry warrant.

- (5) An entry warrant shall be issued if the Judge is satisfied, on the facts alleged in the application concerned that:
 - (a) the entry into the premises is necessary for the purpose of intercepting a postal article or a communication on the premises; and
 - (b) there are reasonable grounds to believe that it would be impracticable to intercept a postal article or communication under the interception direction concerned otherwise than by the use of an interception device on the premises or software on electronic equipment located on the premises.

(6) An entry warrant:

- (a) shall be in the prescribed form;
- (b) shall contain the information referred to in subsection (3) (a) (ii) and (iii); and
- (c) may contain conditions or restrictions relating to the entry upon the premises concerned as the Judge may consider necessary.
- (7) An entry warrant shall permit an authorised officer to enter upon the premises specified in the entry warrant for the purposes of intercepting a postal article or a communication by means of an interception device or software.
 - (8) An entry warrant shall expire when:
 - (a) the period or the extended period for which the related interception direction concerned has been issued lapses; or

- (b) the interception direction to which it relates is terminated in accordance with section 10.
- (9) When an entry warrant has expired pursuant to subsection (8)(a), the authorised officer on whose behalf the application was made or, if he is not available, any other authorised officer who would have been entitled to request the Director of Public Prosecutions to make the application, shall, within two weeks after the date of expiry of the entry warrant, and without applying to a Judge for the issuing of a further entry warrant, remove, or cause to be removed, any interception device which has been installed and which, at the expiry date of the entry warrant, has not yet been removed from the premises concerned.
- (10) An entry warrant shall not be required by a public postal service or a service by means of a public or private communication network for the installation, maintenance, or operation of equipment of software required for the interception of communications or acquisition of protected information or traffic data as permitted under this Act.

Termination of interception direction, etc.

- 10. (1) A Judge who issued an interception direction or an entry warrant, or if he is not available, any other Judge entitled to issue such an interception direction or entry warrant pursuant to section 5 or 9 may:
 - (a) terminate the interception direction or the entry warrant, if:
 - (i) the authorised officer fails to submit a report in accordance with section 12; or
 - (ii) the Judge upon receipt of a report submitted pursuant to section 12 is satisfied that the objectives of the interception direction or the entry warrant, have been achieved, or the

grounds on which the interception direction or the purpose for which the entry warrant was issued, has ceased to exist; or

- (b) terminate the entry warrant and make an order affirming the interception direction if the application for the interception direction and the entry warrant are related and he is satisfied that the interception of communications can be obtained by use only of the interception direction.
- (2) Where a Judge terminates an interception direction or an entry warrant pursuant to subsection (1), he shall forthwith in writing inform the authorised officer concerned of the termination.
- (3) Where an interception direction issued in accordance with this Act is terminated in accordance with subsection (1)(a)(i):
 - (a) the contents of any communication intercepted under that direction shall be inadmissible as evidence in any criminal proceedings or civil proceedings which may be contemplated, unless the Court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise detrimental to the administration of justice; or
 - (b) any postal article that was taken into possession under that direction shall be dealt with in accordance with section 16(3).
- (4) Where an entry warrant is terminated in accordance with this section, the authorised officer shall, within a period of two weeks, after having been informed of the

termination, remove or cause to be removed from the premises to which the entry warrant relates, any interception device which was installed pursuant to the entry warrant.

(5) Where an interception direction has been terminated pursuant to this section, an entry warrant issued pursuant to the interception direction shall also be deemed to be terminated.

Modification of interception direction, etc.

11. A Judge may modify any of the provisions of an interception direction or an entry warrant, at any time, after hearing representations the Director of Public Prosecutions acting on behalf of an authorised officer and if he is satisfied that there is any change in the circumstances, which may make the requested modifications necessary or expedient.

Report on progress. 12. A Judge who has issued an interception direction or an entry warrant, shall at the time of issuance or at any stage before the date of expiry thereof, in writing require the authorised officer, on whose behalf the relevant application was made in respect of the interception direction or the entry warrant, to report to him in writing:

- (a) at such intervals as he determines on:
 - (i) the progress that has been made towards achieving the objectives of the interception direction or the entry warrant or both; and
 - (ii) any other matter which the Judge deems necessary; or
- (b) on the date of expiry of the entry warrant and interception direction concerned, on whether the interception device has been removed from the premises and, if so, the date of such removal.

PART III PROTECTED INFORMATION AND TRAFFIC DATA

13. (1) Except as provided in this section, a person who intentionally intercepts or otherwise acquires protected information or traffic data by means of a communication network commits an offence and, on conviction on indictment, is liable to:

Unauthorised interception of protected information,

- (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;
- (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
- (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.
- (2) A person who intentionally intercepts or otherwise acquires protected information or traffic data in the course of its transmission by means of a communication network for the purpose of commercial benefit, political advantage, or criminal activity commits an offence, and on conviction on indictment, is liable to:
 - (a) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the first instance;
 - (b) a fine of not less than one hundred thousand dollars and not exceeding two hundred thousand

- dollars or to a term of imprisonment not exceeding ten years in the second instance; and
- (c) a fine of two hundred thousand dollars and a term of imprisonment not exceeding ten years in the subsequent instances.
- (3) A person does not commit an offence under subsection (1) if:
 - (a) the protected information or traffic data is intercepted in accordance with a disclosure order issued pursuant to section 14;
 - (b) the protected information or traffic data is stored communication and is acquired in accordance with the provisions of any other law;
 - (c) the interception is made through a communication network that is so configured as to render the protected information or traffic data readily accessible to the general public.
- (4) A person does not commit an offence under subsection (1) where the person is an authorised officer who believes that the interception of protected information or traffic data is necessary for the purpose of an emergency, of preventing damage to public or private property, 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, or in the interests of national security.

14. (1) Where information has come into the possession of an authorised officer by virtue of an interception direction or an entry warrant, pursuant to this Act, or by means of the exercise of a statutory power to seize, detain,

Order requiring disclosure of protected information, etc. inspect, search or otherwise to interfere with documents or other property, or is likely to do so, or has otherwise come into possession of an authorised officer by any other lawful means, and he has reasonable grounds to believe that:

- (a) a key to protected information or traffic data is in the possession of any persons; and
- (b) disclosure of the information or data is necessary for any of the purposes specified in section 6(1)(a);

the Director of Public Prosecutions may apply in the prescribed form on his behalf to a Judge in chambers for a disclosure order requiring the person whom he believes to have possession of the key to provide disclosure in respect of the protected information or traffic data.

- (2) A disclosure order under subsection (1):
 - (a) shall:
 - (i) be in the prescribed form;
 - (ii) describe the protected information or traffic data to which the order relates;
 - (iii) specify the time by which the order is to be complied with, being a reasonable time in all the circumstances; and
 - (iv) set out the disclosure that is required by the order, and the form and manner in which the disclosure is to be made; and
 - (b) require the person to whom it is addressed to keep confidential the contents of the existence of the order.

- (3) In granting a disclosure order required for the purposes of subsections (1) and (2), the Judge shall take into account:
 - (a) the extent and the nature of any protected information or traffic data to which the key is also a key; and
 - (b) any adverse effect that complying with the order might have on a business carried on by a person to whom the order is addressed;

and shall permit only such disclosure as is proportionate to what is sought to be achieved, allowing, where appropriate, for disclosure in such a manner as would result in the putting of the information or data in intelligible form other than by disclosure of the key itself.

- (4) A disclosure order made pursuant to this section shall not require the making of any disclosure to a person other than:
 - (a) the authorised officer named in the disclosure order; or
 - (b) such other person, or description of persons, as may be specified in the disclosure order.

Effects of disclosure.

- 15. (1) A person to whom a disclosure order is addressed:
 - (a) shall use any key in his possession to obtain access to the protected information or traffic data; and
 - (b) in accordance with the disclosure order, shall disclose the protected information or traffic data in an intelligible form.

- (2) When a disclosure order requiring access to protected information or traffic data or the putting of protected information or traffic data into intelligible form, is addressed to a person who is:
 - (a) not in possession of the protected information or traffic data to which the order relates; or
 - (b) incapable, without the use of a key that is not in his possession, of obtaining access to the protected information or traffic data or disclosing it in an intelligible form;

he shall be taken to have complied with the order if he discloses any key to the protected information or traffic data that is in his possession or the identity of the person he knows to be in possession of the protected information or traffic data or a key to the protected information or traffic data.

(3) It shall be sufficient for the purposes of complying with a disclosure order for the person to whom it is addressed to disclose only those keys, the disclosure of which is sufficient to enable the person to whom they are disclosed to obtain access to the protected information or traffic data and to put it in an intelligible form.

(4) Where:

- (a) the disclosure required by a disclosure order pursuant to this section allows the person to whom it is addressed to comply with the disclosure order without disclosing all of the keys in his possession; and
- (b) there are different keys in the possession of the person referred to in paragraph (a), the disclosure of which would constitute compliance with the order;

that person may select which of the keys, to disclose for the purposes of complying with the disclosure order.

- (5) Where a disclosure order is addressed to a person who:
 - (a) was in possession of a key to protected information or traffic data but is no longer in possession of it; and
 - (b) if he had continued to have the key to the protected information or traffic data in his possession, would be required by virtue of the order to disclose it; and
 - (c) is in possession of information that would facilitate the obtaining of discovery of the key to the protected information or traffic data or the putting of the protected information or traffic data into an intelligible form;

that person shall disclose to the person to whom he would have been required to disclose the key, all such information as is mentioned in paragraph (c) for the purpose therein mentioned.

- (6) An authorised officer who obtains a disclosure order shall ensure that such arrangements are made as are necessary for ensuring that:
 - (a) a key disclosed pursuant to the disclosure order is used to obtain access to or put into intelligible form only the protected information or traffic data in relation to which the order was given;
 - (b) every key disclosed pursuant to the disclosure order is stored, for so long as it is retained,

in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the information or put it in an intelligible form; and

- (c) the number of:
 - (i) persons to whom the key is disclosed or otherwise made available; and
 - (ii) copies made of the key;

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

- (7) Subject to subsection (8) of this section, where any relevant person incurs any loss or damage as a consequence of a breach by a person referred to in subsection (6) of the duty imposed upon him by that subsection, the breach shall be actionable against the person referred to in subsection (6) at the suit or instance of the relevant person.
- (8) A person is a relevant person for the purposes of subsection (7) if he is:
 - (a) a person who has made a disclosure in pursuance of a disclosure order made under section 14; or
 - (b) a person whose protected information, traffic data, or key has been disclosed pursuant to a disclosure order made under section 14:

and loss or damage shall be taken into account for the purposes of section 14 to the extent only that it relates to the disclosure of a particular protected information, traffic data or a particular key which, in the case of a person falling within paragraph (b), shall be his information or key.

- (9) For the purposes of subsection (8):
 - (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.

PART IV EXECUTION OF INTERCEPTION DIRECTIONS, ENTRY WARRANTS, ETC.

Execution of interception direction, etc

- 16. (1) If an interception direction or entry warrant has been issued pursuant to the provisions of this Act, an authorised officer may execute the order.
- (2) An authorised officer who executes an interception direction or entry warrant or assists with the execution thereof may intercept, at any place in Belize, any communication in the course of its transmission to which the interception direction applies.
- (3) Where possession has been taken of a postal article pursuant to subsection (2), the authorised officer who executes the interception direction and the entry warrant or assists with the execution 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 return the postal article, if it has not been disposed of in terms of paragraph (a), or cause it to be returned to the postal provider if, in the opinion of the authorised officer concerned:
 - (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 at any such criminal or civil proceedings for purposes of evidence or for purposes or order of the court; and
 - (iii) such postal article may be returned without prejudice to the national security of Belize, public safety, public health or conomic well being of Belize as the case may be.
- 17. (1) If an entry warrant has been issued pursuant to the provisions of this Act, an authorised officer who executes or assists with the execution thereof, may at any time during which the entry warrant is in force, without prior notice to the owner or occupier of the premises specified in the entry warrant, enter the said premises and perform any act relating to the purpose for which the entry warrant has been issued.

Entry on premises for execution of warrant.

- (2) An entry warrant shall not be required by a public postal service or a service by means of a public or private communication network for the installation, maintenance, or operation of equipment of software required for the interception of communications or acquisition of protected information or traffic data as permitted under this Act.
- 18. (1) A person who provides a public postal service or a service by means of a public or private communication network shall take such steps as are necessary to facilitate,

Duty to provide assistance.

within the period of time stipulated in the direction or order, the installation of any equipment or software necessary for the carrying out of interception directions or disclosure order for protected information or traffic data, including providing all technical information necessary for the installation, maintenance, and operation of such equipment and software.

- (2) A person who provides a public postal service or a service by means of a public or private communication network shall take such steps as are necessary to facilitate within the period of time stipulated in the direction or order the execution of an interception direction or disclosure order.
- (3) Where the authorised officer intends to seek the assistance of any person in executing an interception direction, entry warrant, or disclosure order for protected information or traffic data, the Judge shall, on the request of the Director of Public Prosecutions, appearing on behalf of the authorised officer, direct appropriate persons to furnish information, facilities, or technical assistance necessary to accomplish the direction or warrant.
- (4) A person who knowingly fails to comply with his duty under this section or otherwise interferes with the execution of an interception direction, entry warrant, or disclosure order for protected information or traffic data, or interferes with the installation or operation of equipment or software required for the execution of a direction, warrant, or order commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;

- (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
- (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.
- (5) An action shall not be brought in any court against a person for any act done in good faith pursuant to a direction, warrant, or order to provide information, facilities or technical assistance under subsections (1) and (2).
- (6) A person directed to provide assistance by way of information, facilities, or technical assistance pursuant to subsections (1) and (2), shall without delay comply in such a manner that the assistance is rendered:
 - (a) as unobtrusively; and
 - (b) with the minimum interference to the services that such a person or entity normally provides to the party affected by the direction, warrant, or order as can reasonably be expected in the circumstances.
- (7) For the purposes of this section, the provision of information facilities or technical assistance includes any disclosure of intercepted material and related communication data to the authorised officer.
- 19. (1) Where an interception direction, entry warrant, or disclosure order for protected information or traffic data has been issued or renewed, it shall be the duty of every person who may be privy to such information to keep such information confidential:

Penalty for unauthorised disclosure of communication, etc.

- (a) the existence and the contents of the interception direction, entry warrant, or disclosure order for protected information or traffic data;
- (b) the details of the issue of the interception direction, entry warrant, or disclosure order for protected information or traffic data and of any renewal or modification;
- (c) the existence and the contents of any requirement to provide assistance with the giving effect to the interception direction, entry warrant, or disclosure order for protected information or traffic data;
- (d) the identity of the officers involved in the execution of the interception direction, entry warrant, or disclosure order for protected information or traffic data;
- (e) information regarding the equipment or software to be used in the execution of the interception direction, entry warrant, or disclosure order for protected information or traffic data;
- (f) the methods or steps taken pursuant to the interception direction, entry warrant, or disclosure order for protected information or traffic data or of any such requirement; and
- (g) everything in the intercepted material, information, or data.
- (2) A person who makes a disclosure to any person of anything that he is required to keep confidential under subsection (1) commits an offence and, on conviction on indictment, is liable to:

- (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;
- (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
- (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.
- (3) In proceedings against a person for an offence under subsection (2), it shall be a defence for that person to show that the disclosure was confined to a disclosure permitted by the authorised officer and explicitly authorised in writing.
- (4) 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 confined to a disclosure authorised:
 - (a) by the interception direction, entry warrant, or disclosure order for protected information or traffic data or by the person to whom the interception direction or the entry warrant is or was addressed; or
 - (b) by section 18.
- 20. (1) Intercepted or disclosed communication, information or data submitted as evidence in any proceedings pursuant to this Act shall be admissible in evidence in accordance with the *Evidence Act*.

Admissibility of interception communication, etc. CAP. 95

- (2) In admitting into evidence any communication, information, or 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 communication, information or data was obtained of the identity of any party who supplied the data;
 - (b) a statement by the witness that the communication, information or data was obtained by virtue of a direction, warrant, or order under sections 5, 9, or 14 shall be sufficient disclosure as to the source or origin of the communication, information or 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) Any communication, information or data discovered during the execution of an interception direction or entry warrant or through the disclosure of protected information or traffic data may be used in the course of any other investigation or produced as evidence in any other case even if no application for interception direction, entry warrant, or order for disclosure of protected information or communication data was requested for that other investigation or case as long as the initial direction, warrant, or order through which the communication, information or data was discovered was duly authorised as directed in this Act.
 - (4) Any communication, information or data discovered during the execution of an interception direction or entry

warrant or through the disclosure of protected information or communication data between a client and his attorney shall not be produced as evidence in court unless this communication, information or data refers to an offence that has been, is being or may be committed.

- (5) Any communication, information or data discovered during the execution of an interception direction or entry warrant or through the disclosure of protected information or communication data that involves spouses, companions, children, or relatives and which could be considered intimate or personal shall not be produced as evidence in court unless this communication, information or data refers to an offence that has been, is being or may be committed.
- 21. (1) Subject to section 22, no question or evidence shall be asked of any person which in any manner discloses that anything specified in subsection (2) has or may have occurred or is going to occur.

Exclusion of matters from legal proceedings.

- (2) The circumstances referred to in subsection (1) are:
 - (a) the making of an application by the Director of Public Prosecutions on behalf of an authorised officer, for a direction, warrant, or order;
 - (b) the issuance of a direction, warrant, or order; or
 - (c) the imposition of any requirement on any person to provide assistance with giving effect to a direction, warrant, or order.
- 22. Section 21 shall not apply to proceedings before the Court in relation to an offence committed pursuant to the provisions of this Act.

Exception to section 21.

PART V LISTED EQUIPMENT

Council as sole authority on equipment.

- 23. (1) The Council shall be the only agency responsible for authorising the possession, importation, exportation, manufacture, assembly, disassembly, operation, sale, or purchase of any electronic, electromagnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it useful for purposes of the interception of communications and the acquisition of protected information or traffic data.
- (2) Subject to subsection (4) the Council shall, by Order published in the *Gazette*, and one or more national newspaper declare any electronic, electromagnetic, acoustic, mechanical or other instrument or device, the design of which renders it useful for purposes of the interception of communications and the acquisition of protected information or traffic data, to be listed equipment subject to subsection (1).
- (3) An Order under subsection (2) may at any time in like manner be amended or withdrawn.
- (4) The Order to be issued by the Council under subsection (2) shall be published in the *Gazette* and one or more national newspaper within twelve months after the date of commencement of this Act.
- (5) Subject to subsection (7), before the Council exercises the powers conferred under subsection (2), the Council shall cause to be published in the *Gazette* and one or more national newspaper the Order, together with a notice inviting all interested parties to submit in writing and within a specified period, comments and representations in connection with the Order.
- (6) A period not exceeding three months shall elapse between the publication of the Order under subsection (5) and the Order under subsection (2).

- (7) Subsection (5) of this section shall not apply:
 - (a) if the Council, pursuant to comments and representations received in terms of subsection(5) decides to publish an Order referred to in subsection (2) in an amended form; or
 - (b) to any declaration in terms of subsection (2) in respect of which the Council is of the opinion that the public interest requires that it be made without delay.
- 24. (1) Subject to subsection (2) of this section and section 25, a person shall not possess, import, export, manufacture, assemble, disassemble, operate, sell, or purchase any listed equipment.

Prohibition on possession of listed equipment.

- (2) Subsection (1) shall not apply to any authorised officer or any other person who possesses, imports, manufactures, assembles, operates, or purchases listed equipment under the authority of a certificate of exemption issued to him by the Council under section 25.
- 25. (1) The Council may, upon application made by a person in the prescribed form, exempt a person from one or all of the prohibited acts listed under section 24(1) for such period and on such terms as the Council may determine.

Exemptions.

- (2) The Council shall not grant an exemption under subsection (1) unless it 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) of this section shall be granted by issuing to the person concerned, a

certificate of exemption, in the prescribed form in which his name, and the scope, period and conditions of the exemption are specified.

- (4) A certificate of exemption granted pursuant to subsection (3) shall be published in the *Gazette* and shall become valid upon the date of such publication. No such publication shall be required in the case of equipment imported, manufactured, assembled, possessed, operated, or purchased by a law enforcement or security agency operating for or on behalf of the Government and the purpose of which shall be to carry out lawful interceptions under this Act.
- (5) A certificate of exemption may at any time in like manner be amended or withdrawn by the Council.
 - (6) A certificate of exemption lapses upon:
 - (a) termination of the period for which it was granted; or
 - (b) withdrawal pursuant to subsection (5).

Penalty for contravention of section 24.

- 26. (1) A person who contravenes section 24 commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;
 - (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
 - (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.

- (2) A company that contravenes section 24 commits an offence and, on conviction on indictment, is liable to:
 - (a) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars in the first instance;
 - (b) a fine of not less than one hundred thousand dollars and not exceeding two hundred thousand dollars in the second instance; and
 - (c) a fine of two hundred thousand dollars in the subsequent instances.
- (3) A court convicting a person or a company of an offence under subsections (1) or (2) of this section shall in addition to any penalty which it may impose in respect of the offence, declare any 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 company; or
 - (d) the possession of which constituted the offence;

to be forfeited to the Government.

- (4) Any equipment declared forfeited under subsection (3) shall, within a period of one week after the date of declaration of forfeiture be delivered to the Commissioner.
- (5) Any equipment delivered to the Commissioner pursuant to subsection (3) shall, in the case of:

- (a) equipment declared forfeited under subsection(3), be kept by the Commissioner of Police;
 - (i) for a period not exceeding three months with effect from the date of declaration of forfeiture; or
 - (ii) if an application under subsection (8) is made, pending the final decision in respect of any such application has been given; or
- (b) equipment declared forfeited under subsection (3) of this section, be kept by the Commissioner for a period not exceeding thirty days with effect from the date of declaration of forfeiture and shall within a period of one week after the expiry of the period of thirty days referred to be destroyed or declared property of the Government by the Commissioner.

(6) The Commissioner shall:

- (a) within one week after the expiry of the period referred to in paragraph (a) sub-paragraph (i) of subsection (5);
- (b) if the decision referred to in subsection (5)(a)(ii) has been given against the person making the application; or
- (c) if an application referred to in subsection(5)(a)(ii) has been refused;

destroy such equipment in his possession or declare such equipment to be the property of the Government.

(7) A declaration of forfeiture pursuant to subsection(3) shall not affect any right which a person or a company,

other than the convicted person or company, may have to the equipment, if the person or company can show that he has been exempted under section 25 from the relevant prohibited act referred to in section 24 in respect of such listed equipment.

- (8) The Judge may, upon an application made at any time within a period of three months with effect from the date of declaration of forfeiture under subsection (3), by any person or company other than the convicted person or company, who claims that:
 - (a) the equipment declared forfeited under subsection (3) is his or its property; and
 - (b) he or it is a person or company referred to in subsection (9);

inquire into and determine those matters.

- (9) If the Judge under subsection (8) is satisfied that:
 - (a) the listed equipment concerned is the property of the person or company;
 - (b) the person or company concerned is a person or company referred to in subsection (8); and
 - (c) the person or company has legal authority to such equipment pursuant to section 25

the Judge shall set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to the person or company.

PART VI MISCELLANEOUS

False statements.

- 27. A person who makes a statement which he knows to be false in any material particular commits an offence under this Act and, on conviction on indictment, is liable to:
 - (a) a fine of not less than twenty five thousand dollars and not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years in the first instance;
 - (b) a fine of not less than fifty thousand dollars and not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding five years in the second instance; and
 - (c) a fine of one hundred thousand dollars and a term of imprisonment not exceeding five years in the subsequent instances.

Amendment of Schedule. 28. The Minister may, by Order published in the Gazette, amend the Schedule.

Regulations.

- 29. (1) The Minister 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 Act into effect.
- (2) The Minister may make Regulations generally for the better carrying out of the purposes and objects of this Act and in particularly to:
 - (a) prescribe the forms required by this Act;

- (b) provide for the disclosure of intercepted communication; or
- (c) provide for the storage and destruction of intercepted communication.
- 30. The Chief Justice may prescribe a code of conduct for authorised officers and shall include a requirement for manual and electronic records, in the case of electronic lawful interception equipment, to be kept by every agency authorised to conduct lawful interception activities under this Act.

Code of Conduct.

31. A person shall not disclose any information obtained under this Act, except:

Disclosure of information.

- (a) as permitted by the Act;
- (b) in connection with the performance of his duties;or
- (c) where the Attorney-General advises that the disclosure be made to a foreign Government or agency of a foreign Government where there exists between Belize and that foreign Government an agreement for the mutual exchange of that kind of information and the Attorney-General considers it to be in the public interest that such disclosure be made.
- 32. (1) The interception of communications, protected information, or traffic data from any person or communication equipment situated within the boundaries of the Central Prison or any other detention facility throughout the country of Belize may be carried out without the requirement of an interception direction or disclosure order, as otherwise stipulated under this Act, subject to the consent of the Council which shall indicate in writing the

Interception in prisons.

agency or agencies that shall be authorised to carry out such interception.

(2) Notwithstanding the exceptions stipulated in subsection (1), all other provisions outlined in this Act shall apply to the interception of communications, protected information, or traffic data in the Central Prison and other detention facilities in Belize.

Protection for acts done in good faith.

33. An authorised officer shall not be liable for any acts done by him in good faith pursuant to the provisions of this Act.

Commencement.

34. This Act shall come into force on a day to be appointed by the Minister by Order published in the *Gazette*.

SCHEDULE [Section 6(1)(a)(v)]

- 1. Arson
- 2. Blackmail and extortion
- 3. Burglary
- 4. Corruption and illicit enrichment
- 5. Counterfeiting
- 6. Drug trafficking
- 7. Espionage
- 8. Forgery
- 9. Fraud
- 10. Hijacking
- 11. Human smuggling
- 12. Kidnapping or abduction
- 13. Manslaughter
- 14. Membership in a criminal gang
- 15. Money laundering
- 16. Murder
- 17. Rape, sexual assault, unlawful carnal knowledge
- 18. Robbery
- 19. Subversion
- 20. Tax evasion
- 21. Terrorism
- 22. Theft

- 23. Threatening and intimidation
- 24. Trafficking in persons
- 25. Treason
- 26. Unlicensed and prohibited explosives, weapons, and ammunition, etc.
- 27. Attempting or conspiring to commit, aiding, abetting, counselling, or procuring the commission of, an offence falling within any of the preceding paragraphs