INTERCEPTION OF COMMUNICATIONS BILL, 2017

Arrangement of Sections

Section

INTERCEPTION OF COMMUNICATIONS BILL, 2017

A BILL FOR AN ACT TO PROVIDE FOR THE INTERCEPTION OF COMMUNICATIONS AND THE PROVISION OF INFORMATION FOR INTERCEPTION IN THE BAHAMAS AND FOR RELATED MATTERS

Enacted by the Parliament of The Bahamas

PART I - PRELIMINARY

1. Short title and commencement.

(1) This Act may be cited as the Interception of Communications Act, 2017.

(2) This Act shall come into operation on such date as the Minister may appoint by Notice published in the Gazette.

2. Interpretation.

(1) In this Act —

"counsel and attorney" has the meaning given to it under the Legal Profession Act *(Ch. 64)*;

"authorised officer" means —

(a) the Commissioner of Police; or

(b) a person authorised in writing by the Commissioner of Police to act on his behalf;

"Commissioner of Police" means the Commissioner of Police appointed under the Constitution;

"communication" includes—

(a) anything transmitted by means of a postal service including a postal article;

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

(c) 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;

"communications data" means any —

(a) traffic data comprised in or attached to a communication, whether by the sender or otherwise, for the purposes of any postal service or communications network by means of which the communication is being or may be transmitted;

(b) 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 communications network; or

(ii) of any part of a communications network in connection with the provision to or use by any person of any communications service; and

(c) 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 communications service;

"communications network" means any facility or infrastructure used by any person to provide communications services, as well as a network whereby a person can send or receive communication services from anywhere in or out of The Bahamas;

"communications provider" means a person who operates a communications network or who provides a communications service;

"communications service" means any service provided by means of a communications network, whether or not the network is operated by the person providing the service;

"disclosure order" means an order made under section 21, 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;

"entry warrant" means a warrant issued pursuant to section 8 or section 10;

"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; and

(d) diverting of any communication from its intended destination to any other destination;

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 telecommunication network is intercepted;

"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 a customer by a communications 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 communications service and being used by the customer in the ordinary course of business; or

(c) being used by a communications provider in the ordinary course of business;

"interception warrant" means a warrant issued under section 5 or 10;

"internal network" means a communications network which is privately owned and used only to serve the need of the organisation or household by which it is owned;

"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 26; or

(b) a component of equipment referred to in paragraph (a);

"Minister" means the Minister responsible for national security;

"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, or sending it; 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 in one or more of them, namely the collection, sorting, conveyance, distribution and delivery whether in The Bahamas 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 communications;

"protected information" means electronic data which, without a key, cannot 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 The Bahamas;

"terrorist act" is a reference to criminal conduct which constitutes an offence under section 3 of the Anti-Terrorism Act *(Ch. 107).*

(2) For the purposes of this Act —

"the interest of national security" shall be construed as including, but not limited to, the protection of The Bahamas from threats of sabotage, espionage, terrorist acts, terrorism or subversion.

"detecting an offence" shall be taken to include—

(a) establishing by whom, for what purpose, 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,

except that, in relation to the issue, extension or modification of an interception warrant or an entry warrant, it shall not include a reference to gathering evidence for use in any legal proceeding.

PART II - INTERCEPTION OF COMMUNICATIONS

3. Prohibition of interception.

(1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a public postal service or a communications network commits an offence, and is liable on summary conviction to a fine not exceeding fifty thousand dollars or a term of imprisonment not exceeding four years, or to both.

(2) A person does not commit an offence under subsection (1) if —

(a) the communication is intercepted in accordance with an interception warrant issued under section 5 or 10 or an entry warrant issued under section 8 or 10;

(b) subject to subsection (3), that person has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception;

(c) the communication is stored communication and is acquired in accordance with the provisions of any other law;

(d) the communication is intercepted as an ordinary incident to the provision of public postal services or communications services or to the enforcement of any law in force in The Bahamas relating to the use of those services;

(e) the interception is of a communication made through a communications network that is so configured as to render the communication readily accessible to the general public; or

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

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

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

(3) A person does not commit an offence under subsection (1) where —

(a) the communication is one sent by or intended for a person who has consented to the interception; and

(b) the person is an authorised officer who believes that the interception of communication is necessary for the purpose of an emergency, 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 interest of national security; or

(c) a private conversation is originated by more than one person or is intended by the originator thereof to be received by more than one person, a consent to the interception thereof by any one of those persons is sufficient consent for the purposes of this or any other Act.

(4) A court convicting a person of an offence under this section may, in addition to any penalty which it imposes in respect of the offence, order the forfeiture and disposal of any device used to intercept a communication in the commission of the offence.

(5) For the purposes of this section, a communication shall be taken to be in the course of transmission by means of a communications network at any time when the network by means of which the communication is being or has been transmitted is used for storing the communication in a manner that enables the intended recipient to collect it or otherwise have access to it.

4. Application for interception warrant and unauthorised disclosure of application.

(1) An authorised officer who wishes to obtain an interception warrant under the provisions of this Act shall request the Attorney-General to make an application *ex parte* to a judge in chambers on his behalf.

(2) Subject to section 10, an application referred to in subsection (1) shall be in writing 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 warrant;

(d) the ground referred to in section 5(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 warrant is required to be issued;

(h) whether any previous application has been made for the issuing of an interception warrant 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) 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 warrant on a ground referred to in section 5(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.

(4) Where an interception warrant is applied for on the grounds of national security, the application 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 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 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 authorization; or

(b) for renewal of an authorisation.

(7) Any person who discloses the existence of an application for an interception warrant, other than to the authorised officer, commits an offence and is liable on summary conviction to a fine not exceeding twenty thousand dollars or to a term of imprisonment not exceeding two years or to both.

(8) It shall be a defence in any proceedings —

(a) against a person, for the person to show —

(i) that the disclosure was made by or to an counsel and attorney in connection with the giving by the counsel and attorney to any client of his advice about the effect of the provisions of this Act; and

(ii) the person to whom or, as the case may be, by whom a disclosure referred to in subsection (7) was made, was the client or a representative of the client

(b) for an offence under subsection (7), for the person to show that the disclosure was made by a counsel and attorney —

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

(ii) for the purposes of the proceedings.

(9) Subsection (8) shall not apply in the case of a disclosure made with a view to furthering any criminal purpose.

(11) In proceedings against a person for an offence under subsection (7), it shall be a defence for that person to show that the disclosure was confined to a disclosure permitted by the authorised officer.

(12) The Attorney-General shall refuse to make any application under this Act where the Attorney-General does not consider the application to be in the public interest or in the interest of justice.

(13) In any proceedings before a court under this Act the Attorney-General may be represented by counsel and attorney.

5. Issuance of interception warrant.

(1) An interception warrant shall be issued if a judge is satisfied, on the facts alleged in the application under section 4, that there are reasonable grounds to believe that —

(a) obtaining the information sought under the interception warrant is necessary—

(i) in the interest of national security;

(ii) in the interest of public order;

(iii) in the interest of public morality;

(iv) in the interest of public safety;

(v) in the interest of public health;

(vi) for the prevention or detection of an offence, where there are reasonable grounds to believe that such an offence has been, is being or may be committed; or

(vii) for the purpose, in circumstances appearing to the judge to be equivalent to those in which he would issue an interception warrant by virtue of subparagraph (vi), of giving effect to the provisions of any mutual legal assistance agreement; 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 warrant;

(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 interest of the administration of justice to issue the interception warrant.

(2) A judge considering an application may require the authorised officer to furnish such further information as he deems necessary.

6. Scope and form of interception warrant.

(1) An interception warrant shall be in the prescribed form and shall permit the authorised officer to —

(a) intercept, at any place in The Bahamas, 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 communications network, of such communications as are described in the warrant; and

(c) secure the disclosure of the intercepted material obtained or required by the warrant, and of related communications data.

(2) An interception warrant shall authorise the interception of —

(a) communications transmitted by means of a postal service or a public or a private communications network to or from —

(i) one particular person specified or described in the warrant; or

(ii) one particular address so specified and described; and

(b) such other communications, if any as may be necessary in order to intercept communications falling within paragraph (a).

(3) An interception warrant shall specify the identity of the —

(a) authorised officer on whose behalf the application is made under section 4, and the person who will execute the warrant;

(b) person, if known and appropriate, whose communication is to be intercepted; and

(c) postal service provider or the communications provider to whom the warrant to intercept must be addressed, if applicable.

(4) An interception warrant may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Act.

(5) An interception warrant issued under this section may specify conditions or restrictions relating to the interception of communications authorised therein.

(6) For the purposes of this Act, "address" includes a particular set of premises, phone number, e-mail address, internet protocol and postal address.

7. Duration and renewal of interception and entry warrant.

(1) An interception warrant 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 under subsection (2).

(2) A judge may renew an interception or an entry warrant before the expiration of the relevant period, upon an application for the renewal being made by the Attorney-General on behalf of an authorised officer, if satisfied that the renewal of the warrant is justified.

(3) An application for the renewal of a warrant under subsection (2) shall be in writing in the prescribed form and shall be accompanied by an affidavit deposing to the circumstances relied on as justifying the renewal.

(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 an entry warrant is issued, or a person acting on his behalf, that an interception warrant is no longer necessary, he shall cause to be made an application to the Court for the cancellation of the warrant and the court may cancel the warrant.

(5) For the purposes of this section "relevant period" means the period of three months beginning with the date of the issuance of the interception warrant or, in the case of an interception warrant that has been renewed, the date of its latest renewal.

8. Application, issuance, form and scope of entry warrant.

(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 warrant.

(2) Where the Attorney-General—

(a) makes an application under section 4 for an interception warrant on behalf of an authorised officer, the Attorney-General 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 warrant relates; or

(b) made an application under section 4, for an interception warrant on behalf of an authorised officer and the authorised officer on whose behalf the application was made, is not available, any other authorised officer may, at any such stage after the issuance of the interception warrant 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, request the Attorney-General to apply *ex parte* to a judge for the issuance of an entry warrant with respect to the premises to which the interception warrant relates.

(3) Subject to section 9, an application for an entry warrant referred to in subsection (2), shall be in writing and 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) if the application is made in terms of subsection (2)(b), also contain proof that an interception warrant has been issued, and an affidavit setting forth the results, if any, obtained in the interception warrant 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; and

(c) indicate whether any previous application has been made for the issue 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.

(4) Subject to subsections (1) and (5), a judge may upon an application made by the Attorney-General 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 —

(i) of intercepting a postal article or a communication on the premises;

(ii) for installing and maintaining an interception device on; or

(iii) for removing an interception device from, the premises; and

(b) there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception warrant concerned otherwise than by the use of an interception device installed on the premises.

(6) An entry warrant —

(a) shall be in the prescribed form in writing;

(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 —

(a) intercepting a postal article or a communication by means of an interception device;

(b) installing and maintaining an interception device; or

(c) removing an interception device.

(8) An entry warrant shall expire when whichever of the following occurs first —

(a) the period or the extended period for which the related interception warrant concerned has been issued lapses;

(b) it is terminated under section 10 by a judge; or

(c) the interception warrant to which it relates is terminated in accordance with section 9 or 10.

(9) When an entry warrant has expired under 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 Attorney-General to make the application, shall, as soon as practicable 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.

9. Termination of interception or entry warrant.

(1) A judge who issued an interception or an entry warrant or both, or if he is not available, any other judge entitled to issue a warrant pursuant to section 4 or 8 may —

(a) terminate the interception or the entry warrant or both, if —

(i) the authorised officer fails to submit a report in accordance with section 12, if applicable; or

(ii) the judge upon receipt of a report submitted under section 12 is satisfied that the objectives of the interception or the entry warrant or both, have been achieved, or the grounds on which the interception warrant or the purpose for which the entry warrant was issued, or both has ceased to exist; or

(b) terminate the entry warrant and make an order affirming the interception warrant if the application for the interception and the entry warrant are related and he is satisfied that the interception of communication can be obtained by use only of the interception warrant.

(2) Where a judge terminates a warrant under subsection (1), he shall forthwith in writing inform the authorised officer concerned of the termination.

(3) Where an interception warrant issued in accordance with this Act is terminated in accordance with this section or section 10 —

(a) the contents of any communication intercepted under that warrant 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 be detrimental to the administration of justice; or

(b) any postal article that was taken into possession under that warrant shall be dealt with in accordance with section 14(3).

(4) Where an entry warrant is terminated in accordance with this section or section 10, the authorised officer shall, as soon as practicable, after having been informed of the termination, remove or cause to be removed from the premises to which the entry warrant relates, any intercepted device which was installed under the entry warrant.

(5) Where an interception warrant has been terminated under this section or section 10, any related entry warrant shall also be deemed to be terminated.

10. Procedure for urgent applications for interception or entry warrant.

(1) Where a judge is satisfied that the urgency of the circumstances so require, he may dispense with the requirements for a written application and proceed to hear an oral application made by the Attorney-General on behalf of an authorised officer for an interception warrant, or an entry warrant, or both or for a renewal of either an interception or an entry warrant, or both.

(2) An oral application referred to in subsection (1) shall —

(a) contain the information referred to in sections 4(2) and 8(6)(b);

(b) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the authorised officer, justifies the making of an oral application; and

(c) comply with any directives, which may be issued by the judge.

(3) A judge may, on an oral application made pursuant to subsection (1), issue an interception or an entry warrant or both, or a renewal thereof, if he is satisfied that —

(a) there are reasonable grounds to believe that the interception or the entry warrant or both, are necessary; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, for the Attorney-General to make a written application, on behalf of the authorised officer, for the issuing of the interception or the entry warrant or both.

(4) An interception or an entry warrant issued under this section shall have the same scope as an interception or an entry warrant issued under sections 5 and 8.

(5) Where an interception or an entry warrant or both, is issued or renewed under this section, the Attorney-General shall, on behalf of the authorised officer, within seventy-two hours of the time of the issue or, as the case may be, the renewal thereof, submit to the judge a written application and affidavit in accordance with the provisions of sections 4(2), or 8(3), or both as the case may be.

(6) On the expiration of seventy-two hours from the time of the issue or the renewal of the interception or the entry warrant or both under this section, the judge shall review his decision to issue or renew the interception or the entry warrant, or both.

(7) In reviewing his decision under subsection (6), the judge shall determine whether the interception or the entry warrant or both, continues to be necessary under section 5(1) or 8(5).

(8) If under this section, the judge is satisfied that the interception or the entry warrant or both, continues to be necessary, he shall make an order affirming the issue or, renewal of the entry warrant or interception warrant or both.

(9) Where under this section, the judge issues an interception warrant and an entry warrant relating to the interception warrant at the same time, and he is satisfied that in accordance with section 5(1) the interception warrant continues to be necessary, but not the entry warrant, he shall make an order affirming the issue of the interception warrant and terminating the entry warrant.

(10) If the judge is not satisfied that an interception or an entry warrant or both, continues to be necessary, he shall make an order terminating either or both.

(11) Where an interception or an entry warrant issued or renewed under this section is terminated under subsection (10), the interception or the entry warrant shall cease to have effect upon such termination.

(12) Where the issue or the renewal of an interception warrant, is affirmed under subsection (8) of this section, the provisions of section 7 shall apply with respect to its duration as if the date of the order affirming the issue or the renewal of the interception warrant were the date on which the warrant was first issued or, as the case may be, the date of its latest renewal.

(13) Where the issue or renewal of an entry warrant is affirmed under subsection (8), the provisions of section 8(8) shall apply with respect to its duration.

(14) Where an interception warrant is terminated under this section, the entry warrant issued under the interception warrant shall also be deemed to be terminated.

11. Modification of interception or entry warrant.

A judge may modify any of the provisions of an interception warrant or an entry warrant or both, at any time, after hearing representations from the Attorney-General 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.

12. Reports on progress.

A judge who has issued an interception or an entry warrant or both, may 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 or the entry warrant or both, 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 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 warrant concerned, on whether the interception device has been removed from the premises and, if so, the date of such removal.

13. Protection for acts done in good faith.

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

PART III - EXECUTION OF INTERCEPTION AND ENTRY WARRANTS

14. Execution of interception or entry warrant.

(1) If an interception or an entry warrant or both, has been issued under the provisions of this Act, an authorised officer may execute that interception or entry warrant or both.

(2) An authorised officer who executes an interception or an entry warrant or assists with the execution thereof may intercept, at any place in The Bahamas, any communication in the course of its transmission to which the interception warrant applies.

(3) Where possession has been taken of a postal article under subsection (2), the authorised officer who executes the interception 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 interest 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 The Bahamas, public safety, public health or economic well being of The Bahamas as the case may be.

(4) A person referred to in subsection (2) shall take reasonable steps to minimize the impact of the interception on a party who is not the object of the interception.

15. Entry on premises for execution of entry warrant.

If an entry warrant has been issued under 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.

16. Duty to provide assistance.

(1) A person who provides a public postal service or a communications service by means of a public communications network or a private communications network shall take such steps as are necessary to facilitate the execution of an interception or an entry warrant, or both.

(2) Where the authorised officer intends to seek the assistance of any person in executing an interception or an entry warrant or both, the judge may, on the request of the Attorney-General, appearing on behalf of the authorised officer, make an order directing appropriate persons to furnish information, facilities, or technical assistance necessary to accomplish the interception.

(3) A person who knowingly fails to comply with an order under subsection (2) commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars to a term of imprisonment not exceeding six months or to both.

(4) An action shall not be brought in any court against a person for any act done in good faith under an interception or an entry warrant or both, to provide information, facilities or technical assistance under subsection (2).

(5) A person directed to provide assistance by way of information, facilities, or technical assistance pursuant to subsection (2), shall promptly 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 interception or entry warrant, as can reasonably be expected in the circumstances.

(6) For the purposes of this section, the provision of information facilities or technical assistance includes any disclosure of intercepted material and related communications data to the authorised officer.

17. Confidentiality of intercepted communications.

(1) Where a judge issues an interception or an entry warrant, he shall issue such directions as he considers appropriate for the purpose of requiring the authorised officer to make such arrangements as are necessary —

(a) for ensuring that —

(i) the extent to which the intercepted communication is disclosed;

(ii) the number of persons to whom any of that communication is disclosed;

(iii) the extent to which any such communication is copied; and

(iv) the number of copies made of any of the communication,

is limited to the minimum that is necessary for the purposes of the investigations in relation to which the warrant was issued or of any prosecution for an offence; and

(b) for ensuring that each copy made of any of that communication is —

(i) stored in a secure manner for so long as its retention is necessary for such purposes aforesaid; and

(ii) destroyed as soon as its retention is no longer necessary for those purposes.

(2) Where any record is made, whether in writing or otherwise, of any communication obtained by means of a warrant the person to whom the interception or the entry warrant or both, is issued shall, as soon as possible after the record has been made, cause to be destroyed so much of the record as does not relate directly or indirectly to the purposes for which the interception or the entry warrant was issued or is not required for the purposes of any prosecution for an offence.

(3) A person who fails to comply with subsection (2) commits an offence and is liable, on summary conviction, to a fine not exceeding five thousand or to imprisonment for a term not exceeding six months or both.

18. Exclusion of matters from legal proceedings.

(1) Subject to section 19, no evidence shall be adduced, question asked, assertion or disclosure made, or other thing done, for the purposes of or in connection with any legal proceedings which, in any manner —

(a) discloses, in circumstance as are specified in subsection (2) from which the origin of the contents of intercepted communications data may be inferred; or

(b) tends, apart from any such disclosure, to suggest that anything specified in subsection (2) has or may have occurred or is going to occur.

(2) The circumstances referred to in subsection (1) are as follows —

(a) conduct by a person falling within subsection (3) that was or would be an offence under section 3(1);

(b) the issue of an interception or an entry warrant or both;

(c) the making of an application by the Attorney-General on behalf of an authorised officer, for a warrant under the Act;

(d) the imposition of any requirement on any person to provide assistance with giving effect to an interception or an entry warrant.

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

(a) any person to whom an interception or an entry warrant pursuant to this Act may be addressed;

(b) any person holding office under the Crown;

(c) any person employed by or for the purposes of the Royal Bahamas Police Force;

(d) any person providing a postal service or employed for the purposes of any business of providing a postal service; and

(e) any person providing a communications service or an employee for the purposes of any business of providing such a service.

19. Exceptions to section 18.

(1) Section 18 shall not apply to —

(a) any application to a judge under this Act; and

(b) any proceedings for a relevant offence.

(2) Section 18 shall not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the lawfulness of a dismissal on the grounds of any conduct constituting an offence under section 3(1), or section 22.

(3) Section 18(1)(a) shall not prohibit the disclosure of any contents of a communication if the interception of that communication does not constitute an offence by virtue of section 3(2)(b), (c), (d) or section 3(3).

(4) Where any disclosure is proposed to be or has been made on the grounds that it is authorised by subsection (3), section 18(1) shall not prohibit the doing of anything in or for the purposes of, so much of any legal

proceedings as relates to the question whether that disclosure is or was so authorised.

(5) Section 18(1)(b) shall not prohibit the doing of anything that discloses any conduct of a person for which he has been convicted of an offence under section 3(1), 16 or 22.

(6) Nothing in section 18(1) shall prohibit any such disclosure of any information that continues to be available as is confined to a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him by his duty to secure the fairness of the prosecution.

(7) For the purposes of this section **"relevant offence"** means —

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

(b) an offence under the Communications Act (*Ch. 304*);

(c) perjury in the course of any proceedings mentioned in subsection (1) or subsection (2);

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

(e) contempt of court committed in the course of, or in relation to, any proceedings mentioned in subsection (1) or subsection (3).

20. Offence for unauthorised disclosure of interception.

(1) Where an interception or an entry warrant or both, has been issued or renewed, it shall be the duty of every person mentioned under section 18(3) to keep confidential such information as to —

(a) the existence and the contents of the interception and the entry warrant;

(b) the details of the issue of the interception and the entry warrant and of any renewal or modification of either;

(c) the existence and the contents of any requirement to provide assistance with the giving effect to the interception or the entry warrant;

(d) the steps taken under the interception or the entry warrant; and

(e) the contents of the intercepted material together with any related communications 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 is liable on summary conviction to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding one year or to both.

(3) In relation to proceedings against any person for an offence under this section in respect of any disclosure, sections 4(8) to 4(11) shall apply with any necessary modification as they apply in relation to proceedings under section 4.

(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 or the entry warrant or by the person to whom the interception or the entry warrant is or was addressed; or

(b) by section 16.

PART IV - PROTECTED INFORMATION

21. Order requiring disclosure of protected information.

(1) Where protected information has or is likely to come into the possession of an authorised officer by virtue of an interception or an entry warrant or both, under this Act, or by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, 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 the protected information is in the possession of any person; and

(b) disclosure of the information is necessary for the purposes of the investigation in relation to which the warrant was issued,

the Attorney-General may apply in the prescribed form 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.

(2) A order under subsection (1) —

(a) shall —

(i) be in writing in the prescribed form;

(ii) describe the protected information 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;

(iv) set out the disclosure that is required by the order, and the form and manner in which the disclosure is to be made;

(b) may, require the person to whom it is addressed to keep confidential the contents of the existence of the order.

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

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

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

(4) In granting the 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 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 in intelligible form other than by disclosure of the key itself.

(5) An order under this section shall not require the making of any disclosure to a person other than —

(a) the authorised officer named in the order; or

(b) such other person, or description of persons, as may be specified in the order.

22. Effects of disclosure order.

(1) Subject to subsection (2), a person to whom a disclosure order is addressed—

(a) shall be entitled to use any key in his possession to obtain access to the protected information; and

(b) in accordance with the disclosure order, shall disclose the protected information in an intelligible form.

(2) Where a disclosure order requires the person to whom it is addressed to disclose protected information in an intelligible form, that person 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) the disclosure is made in accordance with the order, with respect to the person to whom and the time in which, he was required to disclose the information.

(3) When a disclosure order requiring access to protected information or the putting of protected information into intelligible form, is addressed to a person who is —

(a) not in possession of the protected information 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 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 that is in his possession.

(4) 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 and to put it in an intelligible form.

(5) Where —

(a) the disclosure required by a disclosure order under section 21 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, or combination of 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, or combination of keys, to disclose for the purposes of complying with the order.

(6) Where a disclosure order is addressed to a person who —

(a) was in possession of a key to protected information but is no longer in possession of it; and

(b) if he had continued to have the key to the protected information 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 the putting of the protected information 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).

(7) A person who, without reasonable excuse fails to comply with a disclosure order commits an offence and is liable on summary conviction on indictment to a fine not exceeding twenty thousand or to a term of imprisonment not exceeding one year or to both.

(8) A person who obtains a disclosure order shall ensure that such arrangements are made as are necessary for ensuring that —

(a) a key disclosed under the disclosure order is used to obtain access to or put into intelligible form only the protected information in relation to which the order was given;

(b) every key disclosed under 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.

23. Tipping off.

(1) This section applies where a disclosure order under section 21 contains a provision requiring —

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

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

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

(2) Any person who makes a disclosure to any other person of anything that he is required by a disclosure order under section 21 to keep confidential, commits an offence and is liable, on summary conviction, to a fine not exceeding twenty thousand dollars or to a term of imprisonment not exceeding one year or to both.

(3) 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 —

(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 issued to him or, as the case may be, on becoming aware of it or of its contents, to prevent the disclosure.

(4) Sections 4(8) to 4(10) shall apply, with necessary modifications, in relation to proceedings for an offence under this section as they apply in relation to proceedings for an offence under section 4.

(5) 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 confined to a disclosure authorised —

(a) by the terms of a disclosure order made under section 21; or

(b) by or on behalf of a person who—

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

(ii) came into the possession of that protected information as mentioned in section 21(1).

(6) In proceedings for an offence under this section against a person other than the person to whom the disclosure order under section 21 was addressed, 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 confidential what was disclosed.

PART V - COMMUNICATIONS DATA

24. Disclosure of communications data.

(1) For the purposes of this section —

"designated person" means the Minister or a person designated for the purposes of this section by the Minister by order published in the Gazette;

"traffic data" in relation to a communication, means any communication data —

(a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication 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 communications network for effecting, in whole or in part, the transmission of any communications; or

(ii) any communications 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) Where it appears to the designated person that a communications provider is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the communications provider —

(a) to disclose to an authorised officer all of the data in his possession or subsequently obtained by him; or

(b) if the communications provider is not already in possession of the data, to obtain the data and to disclose the data to an authorised officer.

(3) A designated person shall not issue a notice under subsection (2) in relation to any communications data unless he is satisfied that it is necessary to obtain the data and to disclose the data to an authorised officer so disclose it.

(4) A designated person shall not issue a notice under subsection (2) in relation to any communication data unless he is satisfied that it is necessary to obtain that data —

(a) in the interest of national security;

(b) for the purpose of preventing or detecting any offence, where there are reasonable grounds to believe that such an offence is being or may be committed;

(c) in the interest of public order;

(d) in the interest of public morality;

(e) in the interest of public health;

(f) for the purpose in an emergency, of preventing death, 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

(5) A notice under this section shall state—

(a) the communication data in relation to which it applies;

(b) the authorised officer to whom the disclosure is to be made;

(c) the manner in which the disclosure is to be made;

(d) the matters falling within subsection (3) by reference to which the reference is issued; and

(e) the date on which it is issued.

(6) A notice under this section shall not require —

(a) any communications data to be obtained after the end of the period of one month beginning on the date on which the notice is issued; or

(b) the disclosure, after the end of such period, of any communications data not in the possession of the provider of the communications service, or required to be obtained by him, during that period.

(7) The provisions of sections 21 and 22 shall apply, with necessary modifications, in relation to the disclosure of data pursuant to a notice under this section.

(8) Subject to subsection (8), a provider of a communications service, to whom a notice is issued under this section, shall not disclose to any person the existence or operation of the notice, or any information from which such existence or operation could reasonably be inferred.

(9) The disclosure referred to in subsection (7) may be made to —

(a) an officer or agent of the service provider for the purpose of ensuring that the notice is complied with; or

(b) a counsel and attorney for the purpose of obtaining legal advice or representation in relation to the notice,

and a person referred to in paragraph (a) or (b) shall not disclose the existence or operation of the notice, except to the authorised officer specified in the notice for the purpose of —

(i) ensuring that the notice is complied with, or obtaining legal advice or representation in relation to the notice, in the case of an officer or agent of the service provider; or

(ii) giving legal advice or making representations in relation to the notice, in the case of a counsel and attorney.

(10) A person shall not disclose any communications data obtained under this Act, except —

(a) as permitted by the notice;

(b) in connection with the performance of his duties; or

(c) where the Minister directs that the disclosure be made to a foreign Government or agency of a foreign Government where there exists between The Bahamas and that foreign Government an agreement for the mutual exchange of that kind of information and the Minister considers it to be in the public interest that such disclosure be made.

(11) A person who contravenes subsection (7), (8) or (9) commits an offence and is liable, on summary conviction, to a fine not exceeding twenty thousand dollars or to a term of imprisonment for a term not exceeding one year or to both.

25. Admissibility of communications data.

(1) Subject to sections 18 and 19, and to subsection (2) of this section, communications data obtained in accordance with this Act 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 of the identity of any party who supplied the data;

(b) a statement by the witness that the data was obtained by virtue of a disclosure order under section 21 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 proceeding in respect of an offence under this Act but if the court is satisfied that —

(a) the disclosure is would be likely to jeopardise the course of any investigations or be prejudicial to the interest of national 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 - LISTED EQUIPMENT

26. Listed equipment.

(1) Subject to subsection (4) the Minister shall, by order published in the Gazette, declare any electronic, electro magnetic, acoustic, mechanical or other instrument, device or equipment, as being of a design which renders it primarily useful for purposes of the interception of communications, subject to such conditions or circumstances specified in the order.

(2) The first order to be issued by the Minister under subsection (1) shall be published in the Gazette within four months after the date of commencement of this Act.

(3) Subject to subsection (5), before the Minister exercises the powers conferred by subsection (1), the Minister shall cause to be published in the Gazette a draft of the proposed 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 proposed order.

(4) A period not exceeding one month shall elapse between the publication of the draft order and the publication of the order under subsection (1).

(5) Subsection (3) of this section shall not apply —

(a) if the Minister, after consideration of the 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 in accordance with subsection (1) in respect of which the Minister is of the opinion that the public interest requires that it be made without delay.

(6) An order under subsection (1) shall be subject to affirmative resolution of both Houses of Parliament.

(7) The reference in subsection (1) to any electronic, electromagnetic, acoustic, mechanical or other instrument, device or equipment does not include a reference to a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.

27. Prohibition on manufacture and possession of listed equipment.

(1) Subject to subsection (2) and section 28, 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 by the Minister under section 28.

28. Exemptions.

(1) The Minister 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 27(1) for such period and on such terms as the Minister may determine.

(2) The Minister shall not grant an exemption under subsection (1) unless 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.

(5) A certificate of exemption may at any time in like manner be amended or withdrawn by the Minister.

(6) A certificate of exemption lapses upon —

(a) termination of the period for which it was granted; or

(b) withdrawal under subsection (5).

29. Offence for contravention of section 27.

(1) A person who contravenes or fails to comply with section 27 commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

(2) A court convicting a person of an offence under subsection (1) section shall in addition to any penalty which it may impose in respect of the offence, declare any listed equipment which constituted the offence forfeited.

(3) Any listed equipment or other equipment declared forfeited under subsection (2) shall, as soon as practicable after the forfeiture be delivered to the Commissioner of Police.

(4) Any equipment delivered to the Commissioner of Police pursuant to subsection (3) shall be retained by the Commissioner until after the determination of any appeal against the conviction or of any application made under subsection (6).

(5) A declaration of forfeiture under subsection (2) shall not affect any right which a person, other than the convicted person, may have to the listed equipment, if the person can show that —

(a) he has been exempted under section 28 from the relevant prohibited act referred to in section 27 in respect of such listed equipment; and

(b) he has taken all reasonable steps to prevent its possession by other persons including the convicted person; and

(c) could not reasonably be expected to have known or had no reason to suspect that the listed equipment concerned was in the possession of the convicted person.

(6) A judge may, upon an application to set aside a forfeiture made at any time within a period of one month from the date of declaration of the forfeiture, by a person, other than the convicted person, who claims that—

(a) the listed equipment declared forfeited under subsection (2) is his property; and

(b) he is a person referred to in subsection (7),

inquire into and determine the claim.

(7) If the judge hearing the application under subsection (6) is satisfied that the —

(a) listed equipment concerned is the property of the applicant; and

(b) the applicant satisfies the criteria referred to in subsection (6),

the judge shall set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to the applicant.

PART VII - MISCELLANEOUS

30. False statements.

A person who, in an application under this Act makes a statement which he knows to be false in any material particular commits an offence and is liable upon summary conviction to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both.

31. Regulations.

(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) Without prejudice to the generality of the foregoing, the Minister may make regulations particularly to —

(a) prescribe the forms required by this Act;

(b) provide for the disclosure of intercepted communications; or

(c) provide for the storage and destruction of intercepted communications.

32. Code of conduct.

The Attorney-General may prescribe a code of conduct for authorised officers in carrying out activities under or in relation to this Act.

33. Annual Report.

(1) The Attorney-General shall, within three months, after the end of each year, in relation to the operation of this Act in the immediately preceding year, prepare and cause to be laid in both Houses of Parliament 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 average period for which warrants were given;

(d) the number of warrants refused or revoked by the Court;

(e) the number of applications made for renewals;

(f) the number and nature of inceptions made pursuant to the warrants granted;

(g) the offences in respect of which warrants were granted, specifying the number of warrants given in respect of each of those offences;

(h) the number of persons arrested whose identity became known to an authorised officer as a result of an interception under a warrant;

(i) the number of criminal proceedings 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;

(j) 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 as a result of the investigations;

(k) the number of prosecutions commenced against persons for breach of the provisions of this Act and the outcome of those prosecutions;

(l) a general assessment of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences in The Bahamas; and

(m) any other matter the Attorney-General considers necessary.

(2) The report shall not be the subject of any questions, the answer to which would be a breach of this or any other Act save as provided in the report itself.

34. Savings.

(1) This Act is not to be construed as requiring or prohibiting anonymity or encrypted communications.

(2) This Act does not apply in circumstances which are governed by another law that enables an interception to be carried out in accordance with that law.

35. Costs.

The costs incurred in enabling or the carrying out of an interception procedure shall if not otherwise agreed between an electronic communications provider or the provider of a postal service and the authorised officer be apportioned so that the authorised officer is responsible to reimburse the provider for the direct costs incurred by the latter as regards personnel and administration in relation to the provision of assistance in the execution of an interception or entry warrant.

36. Repeal of Ch. 90.

(1) The Listening Devices Act (Ch. 90) is hereby repealed.

(2) Subsection (1) shall not prejudice any action or process done or being taken in accordance with the provisions of the Listening Devices Act.

OBJECTS AND REASONS

The name of the Bill reflects its principal purpose; that is to enable interception of communications. The Bill seeks to provide a single legal framework within which the interception of communications on public and private systems would be authorised. The Bill provides for the interception of all communications networks, regardless of whether they are licensed as public or not. This will include public telecommunication operators and also Internet providers. The Bill also provides for the interception of communication carried wholly or partly by wireless telegraphy and also encompasses all mail handling systems, which includes all parcel and courier services.

Part I of the Bill provides the preliminary provisions, such as the commencement and interpretation clauses. Under this Part the Bill comes into operation on a day to be fixed by the Minister, by notice published in the Gazette. In the interpretation clause, the term "intercept" includes —

(a) "The aural or other acquisition of the contents of any 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 of a communication by means of a monitoring device;

(c) viewing, examining, or inspecting of the contents of any communication; and

(d) diverting of any communication from its intended destination to any other destination;

and "interception" shall be construed accordingly.".

Also, under Part I "the interest of national security" is to be construed as including but not to be limited to "the protection of The Bahamas from threats of sabotage, espionage, terrorist acts, terrorism or subversion" and the term "terrorist act" is a reference to conduct mentioned in the Anti-Terrorism Act *(Ch. 107).*

Part II of the Bill provides for the interception of communications. Within certain narrow exceptions, clause 3 makes it unlawful to intercept any communication in the course of its transmission by means of a public postal service or a public or a private communications network except where authorised by law. Interception may only take place when the information cannot reasonably be acquired by any other means and each interception or entry warrant is authorised by a judge upon *ex parte* application by the Attorney-General at the request of an authorised officer. The judge has to be satisfied that it is strictly necessary in accordance with clauses 5(1) and 8(5). The Attorney-General also has to be satisfied that it is needed in the public interest or interest

of justice. "Authorised officer" is defined as including the Commissioner of Police or a person authorised in writing by him to act on his behalf.

Pursuant to clause 6, the interception of communication may be carried out by an authorised officer by use of an interception or an entry warrant. An interception warrant permits the authorised officer to—

(a) intercept at any place in The Bahamas any communication in the course of its transmission;

(b) secure the interception in the course of its transmission from an address by means of a postal service or a public or private communications network, of such communications as are described in the interception warrant; and

(c) secure the disclosure of the intercepted material obtained or required by the warrant, and of related communications data.

Under clause 8, an entry warrant authorises the authorised officer to enter upon the premises specified in the warrant for the purposes of;

(a) intercepting a postal article or a communication by means of a monitoring device;

(b) installing and maintaining an interception device; or

(c) removing an interception device.

Clause 7 provides for the expiration and renewal of a warrant. On issue of a warrant unless renewed it ceases after 3 months if not earlier.

Clause 8 of the Bill provides that an entry warrant would not be issued by a judge for the entry upon any premises, unless there exists with respect to the premises in question a related interception warrant. This is taken to mean that the interception warrant is valid in accordance with clause 7. It must be noted that in the Bill, an interception warrant is required in all instances where there is need to intercept any communication; an entry warrant is only required in circumstances where it is believed to be impracticable to intercept a communication under the related interception warrant otherwise than by use of an interception device installed on the premises. An interception warrant can thus exist without an entry warrant; however if an interception warrant is terminated an entry warrant issued pursuant to the interception warrant is also deemed to be terminated.

The Bill requires an interception warrant to specify the identity of the authorised officer on whose behalf the interception warrant is issued and the address of the person whose communication is to be intercepted. This is a way of identifying the communications to be intercepted. An entry direction must specify the name of the authorised officer on whose behalf the entry warrant is issued, the premises in respect of which the entry warrant is required and the specific purpose for which the application is made.

Part III of the Bill provides for the execution of interception warrants and entry warrants. It provides that an authorised officer may execute an interception warrant or an entry warrant in accordance with the provisions of the Bill. This Part also allows the authorised officer, in the case of an entry warrant to enter upon the premises stated in an entry warrant without giving prior notice to the owner or occupier of the premises concerned. Pursuant to clause 16, any person who is requested to provide assistance to an authorised officer by virtue of an interception warrant or an entry warrant and refuses to do so, commits an offence.

Clause 18 has the effect of prohibiting the evidential use of intercepted material gathered under an interception direction or an entry warrant or both. Clause 19 provides for exceptions to that clause. Clause 17, provides for the confidentiality of intercepted material. The intent of that clause and clause 20 is to place strict safeguards on the extent to which intercepted material may be disclosed, copied and retained, requiring each of these to be kept to a minimum.

Part IV of the Bill provides for the disclosure of protected material. Under this Part, where protected information comes into the hands of an authorised officer and he has reasonable grounds to believe the key (code, password, etc) to the protected information is in the possession of a person, and the disclosure is necessary for any purpose pursuant to the Act, he may request the Attorney-General to apply on his behalf for a disclosure order requiring the person who has possession of the key to provide disclosure in respect of the protected information.

Part V of the Bill deals with communications data. The Minister has the power under this Part to designate a person to obtain communications data in the circumstances stated in clause 24.

Part VI of the Bill deals with listed equipment. Under this Part, the Minister may by notice published in the Gazette, declare any electronic, electro-magnetic, acoustic, mechanical or other equipment or device, the design which renders it primarily useful for purposes of the interception of communications, under the circumstances specified in the notice, to be listed equipment. A person is not allowed to manufacture, assemble, possess, sell, purchase or advertise any equipment declared to be listed equipment by the Minister, unless he has an exemption order issued pursuant to clause 28 which enables him to do so. This part also provides for the forfeiture of any listed equipment or other equipment obtained from a person convicted of an offence.

By Part VII, provision is made for penalties for false statements, the power of the Minister to make Regulations and for a code of conduct for authorised officers to be prescribed.