

THE OFFICIAL GAZETTE 7TH AUGUST, 2008
LEGAL SUPPLEMENT - C

BILL No. 19 of 2008

Thursday 7th August, 2008

PARLIAMENT OFFICE
Public Buildings,
Georgetown,
Guyana.

7th August, 2008

The following Bill which will be introduced in the National Assembly is published for general information.

S. E. Isaacs,
Clerk of the National Assembly.



GUYANA

BILL No. 19 of 2008

INTERCEPTION OF COMMUNICATIONS BILL 2008

ARRANGEMENT OF SECTIONS

SECTION

1. Short title and commencement.
2. Interpretation.
3. Prohibition of interception.
4. Application for warrant for interception.
5. Scope of warrant.
6. Issuance, duration and revocation of warrant.
7. Oral application for issuance of warrant in urgent circumstances.
8. Modification of warrants.
9. Protection of authorised officer.

10. Duties of persons providing assistance or telecommunication services.
11. Confidentiality of intercepted communication.
12. Order requiring disclosure of protected communication.
13. Effect of disclosure order.
14. Admissibility of evidence.
15. Offences.
16. Disclosure of communications data.
17. Admissibility of communications data.
18. Amendment of Schedule.
19. Regulations.

SCHEDULE

**A BILL
Intituled**

AN ACT to make provision for the interception of communications, the acquisition and disclosure of data relating to communications and the acquisition of the means by which protected communications may be accessed and placed in an intelligible form and for connected purposes.

A.D. 2008. Enacted by the Parliament of Guyana:-

**Short title and
commencement.**

1. This Act may be cited as the Interception of Communications Act 2008 and shall come into operation on such date as the Minister may, by order, appoint and that date shall in no case be later than three months from the date of enactment.

Interpretation.

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

“authorised officer” means-

- (a) the Commissioner of Police;
- (b) the Commissioner-General of the Guyana Revenue Authority; or
- (c) the Chief of Staff of the Guyana Defence Force;

“disclosure order” means an order under section 12 requiring the disclosure of a protected communication;

“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

4

or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

“intercept”, in relation to a telecommunication, means -

(a) monitoring of transmissions made by fibre optic cable or any other form of wire line, by wireless telegraphy, voice over internet protocol, internet and all other forms of electromagnetic communication to or from the apparatus comprising the systems;

(b) monitoring or modification of, or interference with, the system by means of which the communication is transmitted, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or the intended recipient of the communication, and “interception” shall be construed accordingly;

“key”, in relation to any protected communication, means any key, code, password, algorithm or other data the use of which (with or without other keys)-

(a) allows access to a protected communication; or

(b) facilitates the putting of a protected communication into an intelligible form;

“private communication” means a communication that is transmitted or being transmitted by the sender, to a person intended by the sender to receive it, in circumstances in which it is reasonable for the sender and the intended recipient to expect that the communication will not be intercepted by any person other than the intended recipient, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the intended recipient;

“private telecommunications system” means any telecommunications system that, without itself being a public telecommunications system, is a system in relation to which the following conditions are satisfied-

5

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

(b) there is apparatus comprised in the system which is both located in Guyana and used (with or without other apparatus) for making the attachment to the public telecommunications system;

“protected communication” means any electronic data which, without the key to the communication, cannot, or cannot readily, be accessed or put into an intelligible form;

“public telecommunications system” means a telecommunications system used by any person to provide telecommunications services to the public and includes-

(a) a system where the public can send or receive telecommunications services to or from-

- (i) anywhere in Guyana;
- (ii) anywhere outside of Guyana;

(b) a system commonly known as a public switched telephone system;

“telecommunications” means the transmission of intelligence by means of guided or unguided electromagnetic, electrochemical or other forms of energy, including but not limited to intelligence-

(a) in the form of-

- (i) speech, music or other sounds;
- (ii) visual images, whether still or animated;
- (iii) data or text;
- (iv) any type of signals;

(b) in any form other than those specified in paragraph (a);

(c) in any combination of forms; and

(d) transmitted between persons and persons, things and things or persons and things;

“telecommunications system” means a system of telecommunications or any part thereof where a person or thing can send or receive intelligence to or from any point in Guyana;

“telecommunications service” means a service provided by means of a telecommunications system to any person for the transmission of intelligence from, to or within Guyana;

“terrorism” means any act involving the use or threat of violence by a person, which, by reason of its nature and extent, is calculated to create a state of fear in the public or any section of the public.

(2) In this Act, the interests of national security shall be construed as including, but not limited to, the protection of Guyana from threats to public order or of espionage, sabotage, terrorism or subversion.

Prohibition of
interception.

3. (1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunications system commits an offence and is liable on summary conviction to a fine not exceeding **five million dollars** and to imprisonment for a term not exceeding **three years**.

(2) A person does not commit an offence under this section if-

(a) the communication is intercepted in obedience to a warrant issued by a Judge under section 6;

(b) the communication is not intercepted in obedience to a warrant issued by a Judge under section 6 but on the authority of a designated officer in the case of a national emergency or in responding to a case where approval for a warrant is impracticable having regard to the urgency of the case.

(3) The Court by which a person is convicted of an offence under this section may order that any device used to intercept a communication in the commission of the offence shall be forfeited and disposed of as the Court thinks fit.

(4) For the purposes of subsection (1), a communication shall be taken to be in the course of transmission by means of a telecommunications system at any time when the system by means of which the communication is being or has been transmitted is used for storing the

7

communication in a manner that enables the intended recipient to collect it or otherwise have access to it.

Application
for warrant for
interception.

4. (1) Subject to the provisions of this section, an authorised officer may apply *ex parte* to Judge in Chambers for a warrant authorising the person named in the warrant-

(a) to intercept,
in the course of their transmission by means of a public or private telecommunications system, such communications described in the warrant; and

(b) to disclose the intercepted communication to such persons and in the manner specified in the warrant.

(2) An application for a warrant under this Act shall, subject to section 7, be in writing and be accompanied by-

(a) an affidavit deposing to the following matters-

(i) the name of the authorised officer and the entity on behalf of which the application is made;

(ii) the facts or allegations giving rise to the application;

(iii) sufficient information for a Judge to issue a warrant on the terms set out in section 5;

(iv) the period for which the warrant is requested;

(v) the grounds relied on for the issue of a warrant under subsection (3); and

(vi) if the applicant will be seeking the assistance of any person or entity in implementing the warrant, sufficient information for a Judge so to direct in accordance with section 5(3); and

(b) where a warrant is applied for on the ground of national security, a written authorisation, signed by the Minister responsible for national security, authorising the application on that ground.

(3) A Judge shall not issue a warrant under this Act unless he is satisfied that-

(a) the warrant is necessary-

8

Schedule.

- (i) in the interests of national security; or
 - (ii) for the prevention or detection of any offence specified in the Schedule, where there are reasonable grounds for believing that such an offence has been, is being or is about to be committed;
- (b) information obtained from the interception is likely to assist in investigations concerning any matter mentioned in paragraph (a);
- (c) other investigative procedures-
 - (i) have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the warrant;
 - (ii) are too dangerous to adopt in the circumstances; or
 - (iii) are impracticable, having regard to the urgency of the case; and
 - (d) it would be in the best interest of the administration of justice to issue the warrant.

(4) The records relating to every application for a warrant or the renewal or modification thereof shall be sealed until otherwise ordered by the Court.

(5) A person who discloses the existence of a warrant or an application for a warrant, other than to a person to whom such disclosure is authorised for the purposes of this Act, commits an offence and is liable on summary conviction to a fine not exceeding **five million dollars** and to imprisonment for a term not exceeding **three years**.

Scope of warrant.

5. (1) A warrant shall authorise the interception of-

- (a) communication transmitted by means of a public or private telecommunications system to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from-
 - (i) one particular person specified or described in the warrant; or

9

(ii) one particular set of premises so specified or described; and

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

(2) A warrant shall specify-

(a) the identity, if known, of the person whose communications are to be intercepted;

(b) the nature and location of the telecommunications equipment in respect of which interception is authorised;

(c) a particular description of the type of communications sought to be intercepted, and, where applicable, a statement of the particular offence to which it relates;

(d) the identity of the agency authorised to intercept the communication and the person making the application; and

(e) the period for which it is valid.

(3) Where the applicant intends to seek the assistance of any person or entity in implementing the warrant, the Judge shall, on the applicant's request, direct appropriate persons or entities to furnish information, facilities or technical assistance necessary to accomplish the interception.

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

(5) In this section, "addresses" includes a location, email address, telephone number or other number or designation used for the purpose of identifying telecommunications systems or apparatus.

6. (1) Upon receipt of an application or otherwise as provided by this Act and subject to subsections (2) and (3), a Judge may issue a warrant for such period, not exceeding ninety days (in this section referred to as the initial period), as may be specified therein.

(2) A Judge may -

10

(a) on an application by an authorised officer before the expiration of the initial period; and

(b) if satisfied that a renewal of the warrant is justified in any particular case,

renew the warrant for such period (in this section referred to as the first renewal period), not exceeding ninety days from the date of expiration of the initial period, as he may specify therein.

(3) Where a Judge is satisfied that exceptional circumstances exist which would justify a renewal of the warrant beyond the first renewal period, the Judge may, on an application by an authorised officer before the expiration of that period, renew the warrant for such further period, not exceeding ninety days from the expiration of the first renewal period, as he may specify therein.

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

(5) If, at any time before the end of any of the periods referred to in this section, a Judge is satisfied, after hearing representations made by the authorised officer, that a warrant is no longer necessary as mentioned in section 4 (2), he shall revoke the warrant.

7. (1) Where a Judge is satisfied that the urgency of the circumstances so requires-

(a) he may dispense with the requirements for a written application and affidavit and proceed to hear an oral application for a warrant; and

(b) if satisfied that a warrant is necessary as mentioned in section 4(2), he shall issue a warrant in accordance with this Act.

(2) Where a warrant is issued under this section, the applicant shall, within seventy-two hours of the time of issue thereof, submit to the Judge a written application and affidavit in accordance with the provisions of section 4.

(3) On the expiration of seventy-two hours from the time of issue of a warrant under this section, the Judge shall review his decision to issue the warrant and shall-

Oral application
for issuance of
warrant in certain
circumstances.

11

(a) make an order revoking the warrant if-

(i) he is not satisfied that the warrant continues to be necessary as mentioned in section 4 (2); or

(ii) the applicant fails to submit a written application and affidavit as required by subsection (2); or

(b) make an order affirming the warrant, if satisfied that the warrant continues to be necessary as mentioned in section 4(2).

(4) Where a warrant issued under this section is revoked under subsection (3) (a), it shall cease to have effect upon such revocation.

(5) Where a warrant is affirmed under subsection (3) (b), the provisions of section 6 shall apply with respect to its duration.

Modification
of warrants.

8. A Judge may modify a warrant at any time, after hearing representations from an authorised officer and if satisfied that there is any change in the circumstances which constituted grounds for the issue or renewal of the warrant.

Protection of
authorised
officer.

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

Duties of persons
providing assistance
or
telecommunications
services.

10. (1) Every person who provides a telecommunications service by means of a public or private telecommunications system shall take such steps as are necessary for securing that it is and remains practicable for directions to provide assistance in relation to interception warrants to be imposed and complied with.

(2) Any person or entity directed to provide assistance by way of information, facilities or technical assistance under section 5 (3) shall promptly comply with that direction and in such a manner that the assistance is rendered-

(a) as unobtrusively; and

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

as can reasonably be expected in the circumstances.

12

(3) No action shall be brought in any Court against a person or entity for any act done in good faith in pursuance of a direction to provide information, facilities or technical assistance under section 5 (3).

(4) If a judge issuing a warrant under this Act is satisfied that the operation of a public or private telecommunications system has failed to comply with the warrant for want of any support services for the transmission, switching equipment or any other technical facility or requirement, he may direct that the owner, operator or licensee of the telecommunications system shall, at his own cost, forthwith provide the required support service, install necessary switching equipment or provide the technical facility or requirement, as the case may be, for complying with the warrant to the satisfaction of the Court and the compliance with this subsection shall be deemed to be a condition in the licence granted for the operation of the telecommunication system.

Confidentiality of
intercepted
communication.

11. (1) Where a Judge issues a 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-

13

(i) stored in a secure manner for so long as its retention is necessary for such purposes as 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 authorised officer shall, as soon as possible after that record has been made, cause to be destroyed so much of the record as does not relate directly or indirectly to the purpose for which the warrant was issued or is not required for the purposes of any prosecution for an offence.

Order requiring
disclosure of
protected
communication.

12. (1) Where a protected communication has come into the possession of an authorised officer by virtue of a warrant, or is likely to do so, and the officer has reasonable grounds to believe that-

(a) a key to the communication is in the possession of any person; and

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

the officer may apply 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 communication.

(2) An order under this section shall-

(a) be in writing;

(b) describe the communication to which the order relates;

(c) specify the time by which the order is to be complied with, being a reasonable time in all circumstances; and

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

and any such order may require the person to whom it is addressed to keep secret the contents and existence of the order.

14

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

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

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

(4) In granting the order required for the purposes of subsections (1) and (2), the Judge in Chambers shall take into account-

(a) the extent and nature of any protected communication, in addition to the intercepted communication, 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 the person to whom the order is addressed,

and shall require only such disclosure as is proportionate to what is sought to be achieved, allowing, where appropriate, for disclosure in such manner as would result in the putting of the communication 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; or

(b) such other person as may be specified in the order.

13. (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 communication; and

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

Effect of disclosure order.

(2) Where a disclosure order requires the person to whom it is addressed to disclose a protected communication in an intelligible form, that person shall be taken to have complied with that requirement if-

15

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

(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 communication.

(3) Where an order requiring access to a protected communication or the putting of the protected communication into intelligible form is addressed to a person who is-

(a) not in possession of the protected communication 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 communication or of disclosing it in an intelligible form,

he shall be taken to have complied with the order if he discloses any key to the protected communication that is in his possession.

(4) It shall be sufficient for the purpose of complying with an 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 communication and to put it in an intelligible form.

(5) Where-

(a) the disclosure required by an order allows the person to whom it is addressed to comply with the order without disclosing all of the keys in his possession; and

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

the person may select which of the keys, or combination of keys, to disclose for the purpose of complying with the order.

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

(a) was in possession of the key but is no longer in possession of it;

16

(b) if he had continued to have the key 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 or discovery of the key or the putting of the communication 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 to a fine not exceeding **one million dollars** and to imprisonment for a term not exceeding **six months**.

(8) An authorised officer who obtains a disclosure order shall ensure that such arrangements as are necessary are made for securing that-

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

(b) every key disclosed in pursuance to the 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 communication or put it into 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 communication to be accessed or put into an intelligible form.

(9) An authorised officer who knowingly contravenes subsection (8) commits an offence and is liable on summary conviction to a fine not exceeding **three million dollars** and to imprisonment for a term not exceeding **one year**.

17

Admissibility
of evidence.

14. (1) In this section, "sensitive information" means any information that suggests or tends to suggest-

(a) any of the details pertaining to the method by which the communication was intercepted; or

(b) the identity of any party carrying out or assisting in the interception.

(2) Subject to subsection (3), the contents of a communication that is obtained by interception permitted by section 3 shall be admissible as evidence in any criminal proceedings.

(3) In any criminal proceedings-

(a) no evidence shall be adduced and no question shall be asked of any witness that suggests or tends to suggest the disclosure of sensitive information;

(b) a statement by the witness that the interception of the communication was permitted by virtue of section 3(2) (a), (b), (c), (d), (e) or (f), as the case may be, shall be sufficient disclosure as to the source and origin of the communication; and

(c) in proving the truth of a statement referred to in paragraph (b) the witness shall not be asked to disclose sensitive information.

(4) Subsection (3) shall not apply to any criminal proceedings in respect of an offence under this Act, but if the Court is satisfied that-

(a) the disclosure of sensitive information would jeopardize the course of any investigations being carried out by authorised officers; and

(b) the parties to the proceedings would not be unduly prejudiced,

the Court may exclude such disclosure.

(5) Any information obtained by an interception, which would be privileged if the interception had not been carried out, shall remain privileged to the extent that the information would be privileged if the interception had not been carried out.

Offences.

15. (1) A person who, in an application or affidavit under this Act, makes a statement which he knows to be false in any material particular commits an offence and is liable on

18

summary conviction to a fine not exceeding five million dollars and to imprisonment for a term not exceeding three years.

(2) A person who intentionally discloses the contents of any communication obtained -

(a) by means of a warrant, to a person to whom he is not authorised to disclose the communication; or

(b) in contravention of this Act,

commits an offence and is liable on summary conviction to a fine not exceeding five million dollars and to imprisonment for a term not exceeding three years.

(3) Subsection (2) shall not apply to the disclosure of the contents of any communication obtained by means of a warrant which is made, in any criminal proceedings, to a person charged with an offence or to the attorney-at-law representing that person in those proceedings.

Disclosure of
communications data.

16. (1) In this section-

“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 telecommunications system 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 any data falling within paragraph (a)), which is about the use made by any person-

(i) of any telecommunications system; or

(ii) of any part of a telecommunications system in connection with the provision to or use by, any person of any telecommunications service;

“designated person” means the Minister or any person duly authorised for the purposes of this section by the Minister;

“traffic data”, in relation to a communication, means any data-

19

- (a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;
- (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 telecommunications system for effecting, in whole or in part, the transmission of any communication; or
 - (ii) any telecommunications system 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 computer programme, access to which is obtained or which is run by means of the communication, to the extent only that the file or 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 person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the provider-

- (a) to disclose to an authorised officer all of the data in his possession or subsequently obtained by him; or
- (b) if the provider is not already in possession of the data, to obtain the data and so disclose it.

(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 that data-

- (a) in the interests of national security; or

20

Schedule.

(b) for the prevention or detection of any offence specified in the Schedule, where there are reasonable grounds for believing that-

(i) such an offence has been, is being or is about to be committed; and

(ii) the sender or recipient of any communication, or the subscriber to the telecommunications service, to which the data relates, is the subject of an investigation in connection with the offence.

(4) A notice under subsection (2) shall state-

(a) the communications 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 notice is issued; and

(e) the date on which it is issued.

(5) 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 telecommunications service, or required to be obtained by him, during that period.

(6) The provisions of sections 9 and 10 shall apply, with the necessary modifications, to the disclosure of data pursuant to a notice issued under this section.

(7) Subject to subsection (8), a provider of a telecommunications 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.

(8) The disclosure referred to in subsection (7) may be made to-

21

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

(b) an attorney-at-law 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 or 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 an attorney-at-law.

(9) An authorised officer 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) if the Minister responsible for national security directs such disclosure to a foreign government or agency of such government where there exists between Guyana and such foreign government an agreement for the mutual exchange of that kind of information and the Minister considers it in the public interest that such disclosure be made.

(10) A person who contravenes subsection (7), (8) or (9) commits an offence and is liable on summary conviction to a fine not exceeding five million dollars and to imprisonment for a term not exceeding three years.

17. (1) Subject to subsection (2), communications data obtained in accordance with section 16 shall be admissible as evidence in accordance with the law relating to the admissibility of evidence.

(2) In admitting into evidence any communications data -

(a) no question shall be asked of any witness that suggests or tends to suggest the disclosure of any of the details pertaining to the

22

method by which the data was obtained or the identity of any party who supplied the data;

(b) a statement by the witness that the data was obtained by virtue of an order under section 16 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 would jeopardize the course of any investigations being carried out by authorised officers; and

(b) the parties to the proceedings would not be unduly prejudiced thereby,

the Court may exclude disclosure of the matters referred to in subsection (2) (a).

Amendment of
Schedule.

18. (1) The Minister may, by order, add to or delete from the list of offences contained in the Schedule.

(2) An order made under subsection (1) shall be subject to affirmative resolution of the National Assembly.

Regulations.

19. (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) A person who contravenes any regulation made under subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding one million dollars and to imprisonment for a term not exceeding six months.

SCHEDULE

[Sections 4, 16 and 18]

APPLICABLE OFFENCES

1. **Murder.**
2. **Treason.**
3. **Kidnapping or abduction.**
4. **Money laundering.**
5. **Producing, manufacturing, supplying or otherwise dealing in narcotic drugs and psychotropic substances in contravention of the Narcotic Drugs and Psychotropic Substances (Control) Act 1988 (Act No.2 of 1988).**
6. **Trafficking in narcotic drugs and psychotropic substances in contravention of the Narcotic Drugs and Psychotropic Substances (Control) Act 1988 (Act No.2 of 1988).**
7. **Importation or exportation of any firearm or ammunition in contravention of the Firearms Act (Cap. 16:05).**
8. **Manufacture of or dealing in firearms or ammunition in contravention of the Firearms Act (Cap. 16:05).**
9. **Illegal possession of a weapon, firearm or ammunition contrary the Firearms Act (Cap. 16:05).**
10. **Arson.**
11. **Aiding, abetting or conspiring to commit any of the offences mentioned in paragraphs 1 to 10.**

EXPLANATORY MEMORANDUM

This Bill seeks to make provision for the interception of communications, the acquisition and disclosure of data relating to communications and the acquisition of the means by which protected communications may be accessed and placed in an intelligible form.

Clause 1 sets out the short title and provides for the commencement of the proposed legislation.

Clause 2 defines certain words and expressions used in the proposed legislation. These, *inter alia*, include “authorised officer”, “intercept”, “telecommunications” and “terrorism”. The word “intercept”, in relation to telecommunication, is defined to mean the monitoring of transmissions made by fibre optic cable or other forms of wire lines by wireless telegraphy, voice over internet protocol, internet and all other forms of electromagnetic communication.

Clause 3 prohibits the interception of communications but identifies the exceptions which are acceptable. The exceptions are where –

(a) the communication is intercepted in obedience to a warrant issued by a Judge;

(b) the communication is not intercepted in obedience to a warrant issued by a Judge under section 6 but on the authority of a designated officer in the case of a national emergency or in responding to a case where approval for a warrant is impracticable having regard to the urgency of the case.

It also provides that the Court which convicts a person of illegal interception may order that any device used to intercept a communication be forfeited and disposed of as the Court thinks fit.

Clause 4 provides that an authorised officer may apply *ex parte* to a Judge in Chambers for a warrant authorising the person named in the warrant to intercept a communication and to disclose the intercepted communication in the manner specified in

the warrant. The Judge must, before granting the warrant, satisfy himself that the warrant is necessary, that the information obtained from the interception is likely to assist in investigations, that this would be the best investigative procedure and it would be in the best interest of the administration of Justice to issue the warrant. It also provides that it is an offence for a person to disclose the existence of a warrant or an application for a warrant, other than to a person to whom such disclosure is authorised.

Clause 5 deals with the scope of warrant.

Clause 6 provides for the issuance, duration and revocation of warrants.

Clause 7 provides for the issue of a warrant where the urgency of the circumstances requires that certain requirements for the application of the warrant be dispensed with. However, the applicant must submit the written application and affidavit within seventy-two hours of the grant of the warrant. Upon the submission of the application and the affidavit, the Judge must review his decision and may revoke or affirm the warrant.

Clause 8 provides for the modifications of a warrant and clause 9 states that an authorised officer will not be liable for any act done by him in good faith.

Clause 9 deals with the protection of authorised officers. The authorised officer shall not be liable for any act done by him in good faith under the proposed legislation.

Clause 10 confers a duty on all persons providing a telecommunications service to provide assistance in relation to interception warrants. It also protects the person for any act done in good faith in pursuance of a direction to provide information, facilities or technical assistance.

Clause 11 states that when a Judge issues a warrant, he must issue directions which will ensure that the intercepted communication remains confidential at all times and where the authorised officer obtains communications by means of a warrant but

outside the scope of the warrant, he must as soon as possible after destroy the record that does not relate directly or indirectly to the purpose for which the warrant was issued.

Clause 12 provides that where intercepted communication is in the possession of an authorised officer but that communication is protected and the officer has reasonable ground to believe that a key (code, password, etc. which allows access to the protected communication and places it into an intelligible form) is in possession of a person and that disclosure of the key is necessary for the purposes of the investigation, the officer may apply to a Judge in Chambers for a disclosure order. However, the disclosure order must not be used for the purpose only of generating electronic signatures.

Clause 13 provides that the person to whom a disclosure order is addressed must, in accordance with the order, use any key in his possession to obtain access to the protected communication and disclose it in an intelligible form. However, where the person to whom an order is addressed is not in possession of the protected communication or is incapable of accessing the protected communication he shall be taken to have complied with the order if he discloses any key to the protected communication that is in his possession, but where a person fails to comply without reasonable excuse, that person commits an offence.

Clause 14 states that the content of a communication that is obtained by interception is admissible as evidence in any criminal proceedings.

Clause 15 provides that where a person in an application or an affidavit knowingly makes a false statement, or intentionally discloses the contents of any communication obtained to a person to whom he is not authorised to disclose the communication, that person commits an offence.

Clause 16 provides that where it appears to a designated person, who is the Minister or any person prescribed by him, that a person providing a telecommunication service is in possession of or capable of obtaining any communications data, the

27

designated person may, by notice in writing, require that provider to disclose data in his possession or if not in his possession, to obtain the data and so disclose it.

Clause 17 deals with the admissibility of communications data obtained under clause 16 as evidence.

Clauses 18 and 19 confer power on the Minister to amend the Schedule to the Bill and to make regulations.

The Schedule to the Bill identifies applicable offences which may require an authorised officer or designated person to intercept communications.

A handwritten signature in black ink, consisting of a large, stylized initial 'J' followed by a long, sweeping horizontal line that ends in a small flourish.

Minister of Home Affairs.