



GUYANA

ACT No. 21 of 2008

INTERCEPTION OF COMMUNICATIONS ACT 2008

President,

Bhurat Jagdeo
Bhurat Jagdeo,
President.

2nd December, 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

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 com-
mencement.

1. (1) This Act may be cited as the Interception of Communications Act 2008.

(2) This Act comes into force on such day or days as the Minister may by order appoint.

(3) An order may appoint different days for different telecommunications services, different provisions or different purposes of the same provision.

Interpre-
tation.

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 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 and recording of transmissions conveyed by fibre optic cable or any other form of wire line, by wireless telegraphy, voice over internet protocol, internet, satellite, and all other forms of electromagnetic or electrochemical communication to or from apparatus comprising the system;”
- (b) monitoring and recording or modification of, or interference with, the telecommunication system by means of which the communication is transmitted,

so as to make some or all of the contents of the communication available 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 telecommunication" 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 --

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

"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 --

5

- (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 private or public 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 inter-
ception.

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 purpose 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 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 a Judge in Chambers for a warrant authorising the person named in the warrant -

- (a) to intercept and record 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 form and 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 -

- (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;

Schedule.

(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;

7

- (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 authorized 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
 - (ii) one particular set of premises so specified or described; and
- (b) such other communications (if any) as are 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.

Duration of
warrant.

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 –

- (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.

Oral
application
for issuance
of warrant in
certain cir-
cumstances.

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 –

- (a) make an order revoking the warrant if –

9

- (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 continued 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.

(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.

(5) The evidence given by a technical expert in a court of law on behalf of a person who provides a telecommunication service shall be heard *in camera* to protect the identity of the technical expert.

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 –

- (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 authorized 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.

(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.

Effect of
disclosure 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.

(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 -

- (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;
 - (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,