INTERCEPTION OF COMMUNICATIONS ACT

CHAPTER 15:08

Act
11 of 2010
Amended by
14 of 2010

Current Authorised Pages

Pages (inclusive)	*Authorised by L.R.O.*
1–34	

Note on Subsidiary Legislation

This Chapter contains no subsidiary legislation.

CHAPTER 15:08

INTERCEPTION OF COMMUNICATIONS ACT

ARRANGEMENT OF SECTIONS

SECTION

ARRANGEMENT OF SECTIONS—*Continued*

SECTION

PART III

GENERAL PROVISIONS

CHAPTER 15:08

INTERCEPTION OF COMMUNICATIONS ACT

An Act to provide for and about the interception of communications, the acquisition and disclosure of data relating to communications, the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed and other related matters. 11 of 2010.

*[ASSENTED TO 3RD DECEMBER 2010]

WHEREAS it is enacted by section 13(1) of the Constitution that an Act of Parliament to which that section applies may expressly declare that it shall have effect even though inconsistent with sections 4 and 5 of the Constitution and, if any Act does so declare, it shall have effect accordingly: Preamble.

And whereas it is provided in section 13(2) of the Constitution that an Act of Parliament to which that section applies is one the Bill for which has been passed by both Houses of Parliament and at the final vote thereon in each House has been supported by the votes of not less than three-fifths of all the members of that House:

And whereas it is necessary and expedient that the provisions of this Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution:

PART I

PRELIMINARY

1. This Act may be cited as the Interception of Communications Act. Short title.

**See* section 3 for commencement date of this Act.

Act inconsistent with Constitution.

2. This Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution.

Commencement. 294/2010.

3. This Act took effect on 17th December 2010.

Act binds the State.

4. This Act binds the State.

Interpretation.

5. (1) In this Act—

"authorised officer" means the Chief of Defence Staff, the Commissioner of Police or the Director of the Strategic Services Agency;

"communications" includes anything comprising speech, music, sounds, visual images or data of any description or signals between persons, between a person and a thing or between things or for the actuation or control of any apparatus, and whether or not done in real time;

"disclosure order" means an order under section 15 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 communication, means listening to, monitoring, viewing, reading or recording, by any means, such a communication in its passage over a tele-communications network without the knowledge of the person making or receiving the communication;

"Judge" means a Judge of the High Court;

"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;

"Minister" means the Minister to whom the responsibility for national security is assigned;

"offence" means any offence under this Act or any other offence where the penalty, whether on summary conviction or conviction on indictment, is imprisonment for five years or more, and includes an offence where death, imprisonment for the remainder of a person's natural life or life imprisonment is the penalty fixed by law;

"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 network" means any telecommunications network that, without itself being a public telecommunications network, is a network in relation to which the following conditions are satisfied:

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

(b) it is operated without any interconnection to a public telecommunications network;

"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 network" means a telecommunications network used by any person to provide telecommunications services to the public and includes a network whereby the public can send or receive communications to or from—

(a) anywhere in the State;

(b) anywhere outside of the State,

and includes a network commonly known as a public switched telephone network;

"telecommunications" includes the transmission, emission or reception of signals, writing, pulses, images, sounds or other intelligence of any kind by wire, wireless, optical or electromagnetic spectrum or by way of any other technology;

"telecommunications network" means a system or any part thereof, whether wholly or partly in Trinidad and Tobago or elsewhere, used for the provision of a telecommunications service;

"telecommunications service" means a service provided by means of a telecommunications network to any person for the transmission or reception of communications from, to or within the State without change in the content or form, regardless of the technology used to provide such service;

"terrorist act" has the meaning assigned to it by section 2(1) of the Anti-Terrorism Act. Ch. 12:07.

(2) The functions of an authorised officer under this Act may be exercised by him in person or through an officer authorised by him in writing acting under and in accordance with his general or special directions.

(3) In this Act, "the interest of national security" shall be construed as including the protection of the State from threats of espionage, sabotage, any terrorist act or subversion.

PART II

INTERCEPTION OF COMMUNICATION

Prohibition of interception.

6. (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 network commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars and to imprisonment for seven years.

(2) Notwithstanding any other law, 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 8 or 11;

(b) the communication is intercepted by an authorised officer—

(i) in the interest of national security;

(ii) for the prevention or detection of an offence for which the penalty on conviction is imprisonment for ten years or more, and includes an offence where death, imprisonment for the remainder of a person's natural life or life imprisonment is the penalty fixed by law;

(iii) for the purpose of safeguarding the economic well-being of the State; or

(iv) for the purpose of giving effect to the provisions of any international mutual assistance agreement,

and any communication so intercepted may be used for the purpose of an application under section 8 or 11, but shall not be admissible as evidence in any criminal proceedings;

(c) he has reasonable grounds for believing that the person to whom or by whom the communication is transmitted consents to the interception;

(d) the communication is intercepted as an ordinary incident in the course of employment in the provision of telecommunications services;

(e) the communication is not a private communication;

(f) the communication is a stored communication and is acquired in accordance with any other law; or

(g) the interception is of a communication transmitted by a private telecommunications network and is done by a person who has—

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

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

(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 may think 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 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.

(5) Information lawfully intercepted under this Act is exempt information for the purposes of the Freedom of Information Act. Ch. 22:02.

Possession of interception devices.

7. (1) Subject to subsection (2), a person who possesses, sells, purchases, or manufactures a device or any component thereof, knowing that its design renders it primarily useful for unauthorised interception of private communications, commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for five years.

(2) Subsection (1) does not apply to—

(a) a person in possession of such a device or component under the direction of an authorised officer in order to assist that officer in the course of his duties under this Act;

(b) a person in possession of such a device or component for the purpose of section 6(2);

(c) any other person in possession of such a device or component under the authority of a licence issued by the Minister.

(3) A licence issued for the purpose of subsection (2)*(c)* may contain such terms and conditions relating to the possession, sale, purchase or manufacture of a device or component described in subsection (1) as the Minister may prescribe.

Warrant for interception.

8. (1) Subject to this section, an authorised officer may apply *ex parte* to a Judge 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 network, such communications as are described in the warrant; and

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

(2) A Judge shall not issue a warrant under this section 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 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) having regard to the urgency of the case, are impracticable;

(d) it would be in the best interest of the administration of justice to issue the warrant; and

(e) the interception of communications to be authorised by the warrant is proportionate to what is sought to be achieved by such interception.

(3) An application for a warrant under this section shall, subject to section 11, be in the form set out in Schedule 1 and be accompanied by—

Schedule 1.

Schedule 2.

(a) a declaration in the form set out in Schedule 2 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 9;

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

(v) the grounds relied on for the issue of a warrant under subsection (2); 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 9(3); and

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

(4) A declaration under subsection (3)*(a)* is deemed to be a statutory declaration under the Statutory Declarations Act. Ch. 7:04.

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

(6) 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 purpose of this Act, commits an offence and is liable on summary conviction to a fine of fifty thousand dollars and to imprisonment for three years.

Scope of warrant.

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

(2) A warrant shall authorise the interception of—

(a) communication transmitted by means of a public or private telecommunications network 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 is necessary to intercept in order to intercept communications falling within paragraph *(a)*.

(3) A warrant shall specify—

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

(b) the nature and address of the tele-communications equipment in respect of which interception is authorised;

(c) a 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.

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

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

Duration of warrant.

10. (1) Subject to subsections (2) and (3), a warrant shall be issued for such period as may be specified in it, not exceeding ninety days (in this section referred to as "the initial period").

(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 as he may specify in it (in this section referred to as "the first renewal period") not exceeding ninety days from the date of expiration of the initial period.

(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 as he may specify in it, not exceeding ninety days from the expiration of the first renewal period.

(4) An application for a renewal of a warrant under subsection (2) or (3) shall be in writing and accompanied by a declaration 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 8(2), he shall revoke the warrant.

(6) Notwithstanding subsection (3), an authorised officer may make an application for a new warrant.

Application for warrant in urgent circumstances.

11. (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 a declaration and proceed to hear an oral application for a warrant; and

(b) if satisfied that a warrant is necessary as mentioned in section 8(2), he shall issue a warrant in accordance with this Act.

(2) Where a warrant is issued under this section, the applicant shall, within ninety-six hours of the time of its issue, submit to the Judge the documents specified in section 8(3).

(3) Where an applicant has submitted a written application and declaration in accordance with subsection (2), the Judge shall review his decision to issue the warrant and shall—

(a) make an order revoking the warrant if he is not satisfied that the warrant continues to be necessary as mentioned in section 8(2); or

(b) make an order affirming the warrant, if satisfied that the warrant continues to be necessary as mentioned in section 8(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)*, section 10 shall apply with respect to its duration.

(6) Where an applicant has not submitted a written application and declaration in accordance with subsection (2), the warrant issued under this section ceases to have effect upon the expiration of ninety-six hours.

Modification of warrants.

12. 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.

Duties of persons providing assistance or telecommunications services.

13. (1) Every person or entity who provides a telecommunications service by means of a public or private telecommunications network and all other providers of telecommunications services shall take all steps that are necessary to ensure that prompt assistance can be provided where necessary to comply with interception warrants granted under this Act.

(2) A person or entity directed to provide assistance by way of information, facilities or technical assistance under section 9(4) shall, without delay, 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) Where a person or entity acts in contravention of subsection (1) or (2), then without prejudice to any other action with respect to the contravention which is lawfully available, that person or entity commits an offence and is liable on summary conviction to a fine of one million dollars.

Confidentiality of intercepted communication.

14. 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 purpose of the investigation 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 stored in a secure manner for so long as its retention is necessary for any purpose mentioned in paragraph *(a)*.

Order requiring disclosure of protected communication.

15. (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 purpose of the investigation in relation to which the warrant was issued,

the officer may apply to a Judge for an 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; 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 purpose of subsections (1) and (2), the Judge shall take into account—

(a) the extent and nature of any protected communication, the key to which is the same as that to the intercepted communication; 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.

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

(a) is 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 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 combination 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,

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 of one hundred thousand dollars and to imprisonment for one year.

(8) An authorised officer who obtains a disclosure order shall ensure that such arrangements are made as are necessary 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 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 of two hundred thousand dollars and to imprisonment for two years.

Admissibility of evidence.

17. (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 subsections (3) and (4), the contents of a communication that is obtained by interception permitted by warrant issued pursuant to section 8 or 11 shall be admissible as evidence in any criminal proceedings.

(3) Where a warrant issued in accordance with this Act is revoked in accordance with section 11, the contents of any communication intercepted under that direction shall be inadmissible as evidence in any criminal proceedings which may be contemplated.

(4) 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 6(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.

(5) Subsection (4) 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 jeopardise the course of any investigation being carried out by authorised officers; and

(b) the parties to the proceedings would be unduly prejudiced thereby,

the Court may exclude such disclosure.

Disclosure of communications data.

18. (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 purpose of any telecommunications 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 any data falling within paragraph *(a)*, which is about the use made by any person—

(i) of any telecommunications network; or

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

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

(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 purpose of a telecommunications network for effecting, in whole or in part, the transmission of any communication; or

(ii) any telecommunications 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 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 authorised officer that a person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the authorised officer 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) An authorised officer shall not issue a notice under subsection (2) in relation to any communications data unless he has obtained a warrant under section 8 or 11.

(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 by reference to which the notice is issued; and

(e) the date on which it is issued.

(5) Sections 13 and 14 shall apply, with the necessary modifications, to the disclosure of data pursuant to a notice issued under this section.

(6) Subject to subsection (7), 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.

(7) The disclosure referred to in subsection (6) may be made to—

(a) an officer or agent of the service provider, for the purpose 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.

(8) 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 directs such disclosure to a foreign government or agency of such government where there exists between the State 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.

(9) A person who contravenes subsection (6), (7) or (8) commits an offence and is liable on summary conviction to a fine of three hundred thousand dollars and to imprisonment for five years.

Admissibility of communications data.

19. (1) Subject to subsection (2), communications data obtained in accordance with section 18 shall be admissible as 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 suggests or tends to suggest the disclosure of any of the details pertaining to the method by which the data was obtained or the identity of any party who supplied the data;

(b) a statement by the witness that the data was obtained by virtue of an order under section 15 shall be sufficient disclosure as to the source or origin of the data; and

(c) in proving the truth of a statement referred to in paragraph *(b)*, the witness shall not be asked to disclose any of the matters referred to in paragraph *(a)*.

(3) Subsection (2) shall not apply to any proceedings in respect of an offence under this Act, but if the Court is satisfied that—

(a) the disclosure would jeopardise the course of any investigations being carried out by an authorised officer; and

(b) the parties to the proceedings would be unduly prejudiced thereby,

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

Destruction of records.

20. (1) An authorised officer shall ensure that any record of information obtained from the interception of communications in pursuance of section 8 or 11 that is not related to the objective of the interception is destroyed immediately.

(2) An authorised officer shall ensure that any record of information obtained from the interception of communications in

pursuance of section 8 or 11, being information that relates wholly or partly and directly or indirectly to the objective of the interception is destroyed as soon as it appears that no proceedings, or no further proceedings, will be taken in which the information would be likely to be required to be produced in evidence.

(3) Nothing in subsection (2) shall apply to any record of any information adduced in proceedings in any Court.

(4) Where a warrant issued in accordance with section 11 is revoked or ceases to have effect, any record of information obtained from the interception of communications in pursuance of the warrant shall be destroyed immediately.

(5) An authorised officer who intercepts a communication in pursuance of section 6(2)*(b)* shall ensure that any record of information obtained from the interception that is not related to the objective of the interception is destroyed immediately.

(6) The Commissioner of Police shall consult with the Chief of Defence Staff, the Director of the Strategic Services Agency and, where he considers it appropriate, the Director of Public Prosecutions, prior to the destruction.

(7) A person required to destroy any record of information in accordance with this section who fails to do so commits an offence and is liable to a fine of five hundred thousand dollars and to imprisonment for seven years.

PART III

GENERAL PROVISIONS

Protection of authorised officer.

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

Minister to be informed.

22. The Minister shall be informed—

(a) of an interception under section 6(2)*(b)* within ninety-six hours of the commencement of the interception;

(b) of an application under section 8 by the authorised officer who has made the application as soon as is practicable after the making of the application;

(c) of an application under section 11 by the authorised officer who has made the application within forty-eight hours of the making of the application,

Schedule 3. in the form set out in Schedule 3.

Offences. **23.** (1) A person who, in an application or declaration under this Act, makes a statement which he knows to be false in any material particular commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for three years.

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

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

(b) obtained in the course of the interception of communication to a person to whom he is not authorised to disclose the communication whether the interception occurred prior to or after the commencement of this Act; or

(c) obtained in contravention of this Act,

commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for 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.

(4) A person who intentionally has in his possession communications intercepted under this Act and who is not authorised to have such communications commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and to imprisonment for two years.

(5) A person who intentionally has in his possession communications intercepted under this Act and who is not authorised to have such communications and who discloses such communications commits an offence and is liable on summary conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for three years.

(6) No action shall be brought in any Court against a person or entity for any act done in good faith in pursuance of a warrant under section 8 or 11 or a direction under section 6(2)*(b)* to provide information, facilities or technical assistance.

Annual Report.

24. (1) The Minister shall, within three months, after the end of each year, in relation to the operation of the Act in the immediately preceding year, prepare a report relating to–

(a) the number of warrants applied for to intercept communications;

(b) the number of warrants granted by the Court;

(c) the number of warrants applied for and granted under section 11;

(d) the average period for which warrants were given;

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

(f) the number of applications made for renewals;

(g) the number and nature of interceptions made pursuant to the warrants granted;

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

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

(j) the number of criminal proceedings commenced by the State in which private communications obtained by interception under a warrant were adduced in evidence and the number of those proceedings that resulted in a conviction;

(k) the number of criminal investigations in which information obtained as a result of the interception of a private communication under a warrant was used although the private communication was not adduced in evidence in criminal proceedings commenced by the State as a result of the investigations;

(l) the number of prosecutions commenced against persons under sections 6, 7, 8, 17, 19 and 21 and the outcome of those prosecutions;

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

(n) any other matter he considers necessary.

(2) The Minister shall cause a copy of the report prepared by him under subsection (1) to be laid before both Houses of Parliament within one month after its completion.

Regulations.

25. (1) The Minister may make Regulations to give effect to the purpose of this Act.

(2) Regulations made under subsection (1) shall be subject to negative resolution of Parliament.

Schedules amended. [14 of 2010].

26. The Minister may by Order subject to negative resolution of Parliament, amend any of the Schedules to this Act.

SCHEDULE 1

Section 8(3).

APPLICATION FOR A WARRANT

I, (*Name of Authorised Officer*), Chief of Defence Staff/ Commissioner of Police/Director of Strategic Services Agency* hereby apply to a Judge of the High Court under the Interception of Communications Act (hereinafter referred to as "the Act") for a Warrant under section 8 of the Act.

I pray that the Warrant be issued to authorise (*Name of Person to conduct Interception*) to intercept, in the course of its transmission by means of a public or private telecommunications network, the following communications:

(*Description of Communication*)

And I further pray that the said (*Name of Person*) be authorised to disclose the intercepted communication to [*Name(s) of Person(s)*] in the following manner:

(*Description of Manner*)

This application is supported by a statutory declaration from the Authorised Officer pursuant to section 8(3)*(a)* of the Act.

A draft of the order that the Authorised Officer seeks is also attached.

Dated this ..... day of ....., 20.....

Signed: .....
Authorised Officer

*delete as applicable.

Section 8(3).

SCHEDULE 2

STATUTORY DECLARATION IN SUPPORT OF AN APPLICATION FOR A WARRANT

I, (*Name of Authorised Officer*), Chief of Defence Staff/ Commissioner of Police/Director of Strategic Services Agency* acting herein as an Authorised Officer under the Interception of Communications Act (hereinafter referred to as "the Act") make oath and say as follows:

1. I am an Authorised Officer under the Act, namely ..... (*state portfolio*). Except where I state otherwise, the facts set out herein are based on my personal knowledge.

2. By virtue of section 8 of the Act, I am authorised to make this statutory declaration in support of an application for a Warrant under section 8 of the Act, in respect of communications by an individual known as ..... and in respect of the following method(s) of communication:

[*Specify, in detail, the method of communication (e.g., computer, telephone, etc.)*]

(i) .....

(ii) .....

3. A Warrant is required because (*state facts or allegation giving rise to the application*.)

4. This Court is requested to issue a Warrant on the grounds of ..... [*Note: specify ground(s) under section 8 of the Act on which Court is requested to grant the Warrant*].

5. Further, I believe that a Warrant should be issued by this Court because: [the following information should be stated—

(i) if practical, a description of the nature and location of the facilities from which or 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.]

6. I am informed and verily believe that—

(i) the following investigative procedures were engaged and failed to adequately obtain the evidence required: [*specify investigative procedures, if any and reason why they failed*.] or

(ii) other investigative procedures appear to be unlikely to succeed or appear to be too dangerous for the following reasons: [*specify reasons*.]*

7. If a Warrant is issued by this Court, it will be required for a period of ..... months. [*specify number of months Warrant is to subsist*.

Note: the duration of a Warrant is not to exceed ninety days. A further application will have to be made to the Court for an extension, if necessary.]

8. (1) There has not been any previous application for a Warrant made with respect to this person; or

(2) There has been a previous application for a Warrant made with respect to this person [*specify status of previous application*]. *

9. In the circumstances the applicant requests that a Warrant be granted for a period of ..... months/weeks/days.

I MAKE this declaration conscientiously believing the same to be true and according to the Statutory Declarations Act, Chap. 7:04, and I am aware that if there is any statement in this declaration which is false in fact, which I know or believe to be false or do not believe to be true, I am liable to fine and imprisonment.

Dated this ..... day of ....., 20.....

.....
Authorised Officer

*delete as applicable.

Section 23.

SCHEDULE 3

FORM TO NOTIFY MINISTER

To: Minister of National Security

I, ...
(Name and position)

of .....
(department, division, section or branch)

hereby inform you that I have on .....
(Date)

(a) commenced an interception of .....

.....
[state facts, where interception is under section 6(2)(b)];

(b) made an application for a Warrant in the matter of .....

.....
(state facts, where interception is under section 8);

(c) made an oral application for a Warrant in the matter of .....

.....
(state facts, where interception is under section 11).

Dated this ..... day of ....., 20.....

.....
Signature