

2025-08-08

Bill as amended

OBJECTS AND REASONS

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

Arrangement of Sections

PART I

PRELIMINARY

1. Short title
2. Interpretation
3. Construction
4. Act binds the State

PART II

INTERCEPTION OF COMMUNICATION

5. Prohibition of interception
6. Possession of interception devices
7. Warrant for interception
8. Scope of warrant
9. Duration of warrant
10. Application for a warrant in urgent circumstances
11. Modification of warrants

- 12. Revocation of warrant
- 13. Report on progress
- 14. Final report

PART III

EXECUTION OF INTERCEPTION

- 15. Duties of persons providing assistance or telecommunications services
- 16. Entry on premises for the execution of an interception warrant.
- 17. Confidentiality of intercepted communication
- 18. Order requiring disclosure of protected communication
- 19. Effect of disclosure order
- 20. Admissibility of evidence
- 21. Disclosure of communications data
- 22. Admissibility of communications data
- 23. Privileged information
- 24. Destruction of records

PART IV

INDEPENDENT MONITORING COMMISSION

- 25. Establishment of Independent Monitoring Commission

- 26. Functions and powers of the Commission
- 27. Disclosure of interests
- 28. Confidentiality
- 29. Experts
- 30. Staff
- 31. Funds of the Commission

PART V

MISCELLANEOUS

- 32. Protection of authorised officer
- 33. Offences
- 34. Annual Report
- 35. Regulations
- 36. Amendment of *Schedules*
- 37. Commencement

FIRST SCHEDULE

Offences

SECOND SCHEDULE

Independent Monitoring Commission

BARBADOS

A Bill entitled

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 the protected communications may be accessed and placed in an intelligible form and for connected purposes.

ENACTED by the Parliament of Barbados in accordance with provisions of section 49 of the *Constitution* as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Interception of Communications Act, 2025*.

Interpretation

2.(1) In this Act,

“authorised officer” means

- (a) the Commissioner of Police;
- (b) the Director General of the Anti-Corruption and Anti-terrorism Agency;

“Commission” or “Independent Monitoring Commission” means the Commission established under section 25;

“disclosure order” means an order under section 18 requiring the disclosure of a protected communication;

“electronic signature” means anything in electronic form which is

- (a) incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;
- (b) generated by the signatory or other source of the communication or data; and
- (c) 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 telecommunications network without the knowledge of the person making or receiving the communication;

“Judge” means the Chief Justice or a Judge assigned by the Chief Justice;

“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 responsible for interception of communications;

“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 purposes of the communication in question, to a public telecommunications network; and

(b) there is apparatus comprised in the network which is both located in Barbados and used (with or without other apparatus) for making the attachment to the 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 telecommunications services to or from

(a) anywhere in Barbados;

(b) anywhere outside of Barbados

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 Barbados 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;

“terrorism” has the meaning assigned to it by section 3 of the *Anti-Terrorism Act*, Cap. 158.

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

Construction

3.(1) Nothing in this Act shall be construed as being in derogation with section 11(b) and (c) of the *Constitution* to the extent that the provisions of this Act are applied in the interests of national security and law enforcement.

(2) Where there is any conflict between the provisions of this Act and any other enactment, the provisions of this Act shall prevail.

Act binds the State

4. This Act binds the State.

PART II

INTERCEPTION OF COMMUNICATION

Prohibition of interception

5.(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 \$500 000 dollars or to a term of imprisonment of 7 years or to both.

(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 7 or 10;
- (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 set out in the *First Schedule*;

- (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 7 or 10, 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.

Possession of interception devices

6.(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 \$250 000 dollars or to a term of imprisonment of 5 years or to both.

(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 7(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 by regulations prescribe.

Warrant for interception

7.(1) An authorised officer may apply *ex parte* to a Judge for a warrant authorising the person named in the warrant

- (a) to intercept 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 set out in the *First 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) 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 be, subject to section 10, in writing and accompanied by

- (a) an affidavit deposing to the following matters
 - (i) the name of the authorized 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 8;

- (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 8(5); and
- (b) where a warrant is applied for on the ground of national security, a written authorization, signed by the Minister, authorizing the application on that ground.
- (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, in an application or affidavit under this Act, makes a statement which he knows to be false in any material particularity commits an offence and is liable on summary conviction to a fine of \$200 000 or to a term of imprisonment not exceeding 2 years, or to both.

Scope of warrant

8.(1) A warrant shall be issued in writing and shall permit the authorised officer to

- (a) intercept communication during its transmission;
- (b) order a communication provider to intercept the communication during its transmission;
- (c) execute the interception by means of communication networks or communication service providers as described in the interception warrant;
- (d) disclose the interception communications obtained or required by the interception warrant to such persons and in such manner as may be specified in the interception warrant.

- (2) A warrant shall authorise the interception of
 - (a) communications transmitted by communications networks or providers to or from
 - (i) a particular individual specified in the interception warrant;
 - (ii) a particular address specified in the interception warrant.
 - (b) communications transmitted by communications networks or providers from a particular connection specified in the interception warrant;
 - (c) such other communication if any as may be necessary in order to intercept communication falling under paragraph (a).
- (3) A warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept communications specified in the warrant.
- (4) A warrant shall
 - (a) specify the identity of the authorised officer on whose behalf the application is made;
 - (b) identify the person who will execute the interception warrant;
 - (c) identify the communications provider to whom an interception warrant should be addressed and specify if the communications provider shall be authorised to intercept communications, if applicable; and
 - (d) authorise entry on premises under subsection (3) specifying
 - (i) whether the entry is authorised to be made at any time of the day or night or only during specified hours;
 - (ii) any additional measures that are to be taken to secure and exercise the entry on the premises.
- (5) Where the applicant for a warrant 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.

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

(7) A warrant may specify conditions or restrictions relating to the interception of communications authorised therein.

Duration of warrant

9.(1) Subject to subsections (2) and (3), a warrant shall be issued for such period as may be specified in it, not exceeding 120 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 therein (in this section referred to as the first renewal period) not exceeding 120 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 authorized officer before the expiration of that period, renew the warrant for such further period as he may specify therein, not exceeding 120 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 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 authorized officer, that a warrant is no longer necessary he shall revoke the warrant.

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

Application for a warrant in urgent circumstances

10.(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 7(2), he shall issue a warrant in accordance with this Act

(2) Where a warrant is issued under this section, the applicant shall, within 72 hours of the time of issue thereof, submit to the Judge a written application and affidavit in accordance with section 7.

(3) On the expiration of 72 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
 - (i) he is not satisfied that the warrant continues to be necessary as mentioned in section 7(2); or
 - (ii) the applicant fails to submit a written application and affidavit as required by section 7(1) and (3); or
- (b) make an order affirming the warrant, if satisfied that the warrant continues to be necessary as mentioned in section 7(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 9 shall apply with respect to its duration.

Modification of warrants

11. 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.

Revocation of warrant

12.(1) A judge who issued a warrant or, if he is not available, any other judge entitled to issue such a warrant may revoke the warrant, where

- (a) the authorised officer fails to submit a report in accordance with section 13, if applicable;
- (b) the judge upon receipt of a report submitted pursuant to section 13 is satisfied that the objectives of the warrant have been achieved;
- (c) the grounds on which the interception warrant was issued have ceased to exist;
- (d) the conditions of the application referred to in section 7(2) have changed in a way that an application would not be possible anymore.

(2) Where a judge revokes an interception warrant pursuant to subsection (1), he shall forthwith in writing inform the authorised officer concerned of the revocation.

(3) Where a warrant is revoked under subsection (1),

- (a) an authorised officer shall, as soon as practicable, after having been informed of the revocation, remove or cause to be removed from the premises to which the interception warrant relates under section 8(3), any intercepted device which was installed.

- (b) the contents of any communication intercepted under that warrant shall be inadmissible as evidence in any criminal proceedings or civil proceedings which may be contemplated, unless the Court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise detrimental to the administration of justice.

Report on progress

13.(1) A judge who has issued a warrant, may at the time of issuance thereof, or at any stage before the date of expiry thereof, in writing require the authorised officer on whose behalf the relevant application was made in respect of the warrant, to report to him in writing on

- (a) the progress that has been made towards achieving the objectives of the interception warrant; and
- (b) any other matter which the judge considers necessary.

(2) The report under subsection (1) shall also be submitted to the Independent Monitoring Authority for monitoring and assessment purposes.

Final report

14.(1) As soon as practicable after a warrant has expired, the authorised officer who applied for it, shall make a written report to the judge who granted the interception warrant, or if that judge is unable to act to another judge, on the manner in which the power conferred by the interception warrant has been executed and the results obtained by the execution of that power.

(2) A report made for the purposes of subsection (1) shall contain the following information:

- (a) where the interception device was placed;
- (b) the number of interceptions made by means of the interception device;
- (c) whether any relevant evidence was obtained by means of the interception device;

- (d) whether any relevant evidence has been, or is intended to be used in any criminal proceedings; and
 - (e) whether any records of a communication intercepted pursuant to the interception warrant have been destroyed in accordance with section 24 and, if not, why they have not been destroyed.
- (3) The report under subsection (1) shall also, soon as practicable after a warrant has expired, be submitted to the Independent Monitoring Authority for monitoring and assessment purposes.

PART III

EXECUTION OF INTERCEPTION

Duties of persons providing assistance or telecommunications services

15.(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 an entity directed to provide assistance by way of information, facilities or technical assistance under section 8(5) 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 \$200 000.

Entry on premises for the execution of an interception warrant.

16. Where a warrant contains permission to enter on premises pursuant to section 8(3), an authorised officer may at the time specified in the interception warrant enter the premises and perform acts that he is authorised to perform in accordance with the warrant.

Confidentiality of intercepted communication

17. 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

18.(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

- 19.(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 \$100 000 or to a term of imprisonment of one year or to both.

(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 authorized officer who knowingly contravenes subsection (8) commits an offence and upon summary conviction shall be liable to a fine not exceeding \$250 000 or to imprisonment for a term of one year or to both.

Admissibility of evidence

20.(1) Subject to subsections (3) and (4), the contents of a communication that is obtained by interception permitted by warrant issued pursuant to section 7 or 10 shall be admissible as evidence in any criminal proceedings.

(2) Where a warrant issued in accordance with this Act is revoked in accordance with section 10(3)(a), the contents of any communication intercepted under that direction shall be inadmissible as evidence in any criminal proceedings which may be contemplated.

(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 5(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 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.

(5) For the purposes of 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.

Disclosure of communications data

21.(1) 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.

(2) 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 7 or 10.

(3) 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.

(4) Sections 18 and 19 shall apply, with the necessary modifications, to the disclosure of data pursuant to a notice issued under this section.

- (5) Subject to subsection (6), 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.
- (6) The disclosure referred to in subsection (5) 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.
- (7) A person referred to in subsection (6) shall not disclose the existence or operation of the notice, except to the authorised officer specified in the notice or for the purpose of
- (a) obtaining legal advice or representation in relation to the notice, in the case of an officer or agent of the service provider; or
 - (b) 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 (5), (6), (7) or (8) commits an offence and is liable on summary conviction to a fine of \$300 000 and to a term of imprisonment of 5 years or to both.

(10) 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 of any
 - (i) 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.

Admissibility of communications data

22.(1) Subject to subsection (2), communications data obtained in accordance with section 21 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 18 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).

Privileged information

23. Where information has been obtained by interception of communication which has been privileged by any other law relating to

- (a) medical records;
- (b) legal professional privilege; or
- (c) any other information protected by the law relating to privacy or confidentiality,

such information shall remain privileged and shall not be given in any court, except with the consent of the person entitled to waive that privilege.

Destruction of records

24.(1) An authorised officer shall ensure that any record of information obtained from the interception of communications in pursuance of section 7 or 10 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 7 or 10, 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 10 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 5(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) 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 to a fine of \$100 000 or to a term of imprisonment of one year or to both.

PART IV

INDEPENDENT MONITORING COMMISSION

Establishment of Independent Monitoring Commission

25.(1) There is established a Commission to be known as the Independent Monitoring Commission.

(2) The *Second Schedule* has effect with respect to the constitution of the Commission and otherwise in relation thereto.

Functions and powers of the Commission

26.(1) The Commission shall be responsible generally for the monitoring and supervision of the interception of communications to ensure that such interception is conducted in accordance with this Act.

(2) The Commission may on

(a) the basis of the

(i) Report on Progress submitted under section 13; or

(ii) Final Report submitted under section 14; or

(b) its own initiative

carry out any investigation that it considers necessary or desirable in connection with the interception of communications to ensure that such interception is conducted in accordance with this Act.

- (3) The Commission, for the purpose of the investigation under subsection (2),
- (a) may, after notifying the authorised officer or a person or an entity providing assistance pursuant to section 8(5), enter at any reasonable time premises occupied by the agency;
 - (b) is entitled to have full and free access at all reasonable times to all records of the authorised officer or a person or an entity providing assistance pursuant to section 8(5) related to the interception;
 - (c) is entitled to make copies of, and to take extracts from, records of the authorised officer or a person or an entity providing assistance pursuant to section 8(5); and
 - (d) may require an authorised officer or a person or an entity providing assistance pursuant to section 8(5), to give the Commission such information as it considers necessary, being information that is in the officer's or person's possession, or to which the officer or person has access, and that is relevant to the inspection.
- (4) The authorised officer or a person or an entity providing assistance pursuant to section 8(5), shall ensure that the agency's officers provide to the Commission such assistance in connection with the performance or exercise of the Commission's functions or powers under this section as the Commission reasonably requires.
- (5) Where as a result of investigations under subsection (2) Commission determines that there is a breach of this Act, he may issue an enforcement notice which shall require an authorised officer or a person or an entity providing assistance pursuant to section 8(5)
- (a) stop the activity which contravenes the Act; or
 - (b) modify the activity to bring it into compliance with the Act within a period to be stated in the notice.
- (6) Where an authorised officer or a person or an entity providing assistance pursuant to section 8(5) fails to comply with the enforcement notice under (3)

within 14 days after the notice is received, the Commission may make an application to the High Court to enforce the notice.

(7) An authorised officer may appeal to the High Court against a decision of the Commission.

(8) The Commission shall prepare an annual report on the monitoring of communications interception pursuant to section 34.

Disclosure of interests

27. A Commissioner who has any interests in any matter or concern with which the Commission proposes to make decision shall disclose such interests and the nature thereof, and such disclosure shall be recorded in the minutes of the Commission and such Commissioner shall take no part in any deliberation or discussion of the Commission relating to such decision nor shall the Commissioner vote thereon.

Confidentiality

28.(1) A Commissioner or any other person retained to assist the Commission shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commission has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commission authorises that person to release the information.

(2) Any person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to imprisonment for a term of 2 years, or to both.

Experts

29.(1) The Commission may appoint or engage persons having special or technical knowledge to assist the Commission in carrying out its functions.

(2) A person engaged pursuant to subsection (1) shall receive such remuneration as the Commission determines.

Staff

30. The Commission may appoint and employ such other officers and employees as it deems necessary, on such terms and conditions as it thinks fit.

Funds of the Commission

31.(1) The funds and resources of the Commission shall consist of

- (a) such amounts as may be voted for the purpose by Parliament
- (b) all other amounts which may become payable to or vested in the Commission in respect of any matter incidental to its functions.

(2) The funds of the Commission shall be applied to defray the following expenditure

- (a) salaries, fees, allowances and other payments due to the staff of the Commission;
- (b) capital and other operating expenses including maintenance and insurance of any property of the Commission;
- (c) any other expenditure authorised by the Commission in the discharge of its duties, functions and contractual obligations; and
- (d) any other expenses authorised to be spent in the functioning of the Commission.

PART V

MISCELLANEOUS

Protection of authorised officer

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

Offences

33.(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 \$250 000 or to a term of imprisonment of 3 years or to both.

- (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 \$250 000 or to a term of imprisonment of 3 years or to both.

(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 \$100 000 or to a term of imprisonment of one year or to both.

(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 \$250 000 or to a term of imprisonment of 3 years or to both.

(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 7 or 10 or a direction under section 8(5) to provide information, facilities or technical assistance.

Annual Report

34.(1) The Commissioner of Police 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 10;
- (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 destruction of records pursuant to section 24;
 - (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 the Commissioner of Police considers necessary.
- (2) The Commissioner of Police shall submit the report referred to under subsection (1) to the Independent Monitoring Commission for the purpose of assessment of the general operation of the Act.
- (3) The Independent Monitoring Commission shall submit to the Minister such recommendations as it sees fit based on the report referred to under subsection (1).

Regulations

- 35.(1) The Minister may make regulations to give effect to this Act.
- (2) Regulations made under subsection (1) shall be subject to negative resolution.

Amendment of *Schedules*

- 36.(1) The Minister may by order amend the *First Schedule* and *Second Schedule*.

- (2) An order made under subsection (1) shall be subject to negative resolution.

Commencement

- 37.** This Act shall come in to operation on a date fixed by Proclamation.

FIRST SCHEDULE

(Sections 5,7, and 36)

Offences

1. Murder.
2. Treason.
3. Terrorism.
4. Trafficking in persons.
5. Kidnapping or abduction.
6. Money Laundering
7. Producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the *Drug Abuse (Prevention and Control) Act*, Cap. 131.
8. Transporting or storing a dangerous drug where possession of such drug contravenes the *Drug Abuse (Prevention and Control) Act*, Cap. 131.
9. Importing or exporting a dangerous drug in contravention of the *Drug Abuse (Prevention and Control) Act*, Cap. 131.
10. Importation, exportation or transshipment of any firearm or ammunition in contravention of the *Firearms Act*, Cap. 179.
11. Manufacture of or dealing in, firearms or ammunition in contravention of the *Firearms Act*, Cap. 179.

12. Illegal possession of a prohibited weapon or any other firearm or ammunition in contravention of the *Firearms Act*, Cap. 179.
13. An offence under the *Prevention of Corruption Act, 2021* (Act 2021-24).
14. Arson
15. An offence for which the penalty on conviction is imprisonment for 10 years or more.
16. Aiding, abetting, or conspiring to commit any of the offences referred to in paragraphs 1 to 15.

SECOND SCHEDULE

(Section 25)

Independent Monitoring Commission

Composition

1.(1) The Commission shall be comprised of 3 Commissioners, one of whom shall be

- (a) a retired judge;
- (b) a member of civil society; and
- (c) a person nominated by the President.

(2) A Commissioner may be a national selected from a Member State of the Community.

(3) For the purposes of this paragraph

“Community” means the Caribbean Community established by the Treaty; and
 “Treaty” means the Revised Treaty of Chaguaramas establishing the Caribbean Community including the CARICOM Single Market and Economy

- (a) that was signed in the Bahamas on 5th July, 2001; and
- (b) to which Barbados is a party.

Appointment

2. The Commissioners shall be appointed by the President by an instrument in writing for a period of 3 years and shall be eligible for re-appointment.

Remuneration

3. The Commissioners shall receive such remuneration as the President shall determine.

Chairman

4. The Chairman shall be chosen from among the number of Commissioners.

Temporary appointment

5.(1) Where a Commissioner

- (a) is precluded by the Commission from taking part in an investigation or deliberation pursuant to section 27; or
- (b) is unable to act by reason of illness, absence from Barbados or any other reason

the President may appoint a person to act as a Commissioner in his place for that investigation or deliberation or until the termination of the disability.

(2) The President shall fix the remuneration of the person so appointed.

(3) Any person so appointed may complete any unfinished business of the Commission in which he has taken part, even if the Commissioner in whose place he was acting is now able to act.

Resignation

6.(1) A Commissioner other than the Chairman or Chief Executive Officer may at any time resign his office by instrument in writing addressed to the Chairman, who shall forthwith cause the same to be forwarded to the President; and upon the date of receipt by the Chairman of such instrument, the Commissioner ceases to be a member of the Commission unless some other date is mentioned in the instrument.

(2) The Chairman may at any time resign his office by instrument in writing addressed to the President; and upon the date of receipt by the President of such instrument, the Chairman ceases to be Chairman and a Commissioner unless some other date is mentioned in the instrument.

Vacancy

7.(1) A vacancy arises in the membership of the Commission on the death or resignation of a Commissioner.

(2) Where a vacancy arises or membership of the Commission is terminated in accordance with subparagraph (1) or paragraph 6 or 8, a person may be appointed in accordance with paragraph 2 to fill that vacancy.

(3) Where a vacancy arises or membership of the Commission is terminated in accordance with subparagraph (1) or paragraph 6 or 8, the remuneration of that person may be made in accordance with paragraph 3.

Termination

8. The President may terminate the appointment of any Commissioner if that Commissioner

- (a) fails to disclose his interest in accordance with section 27;
- (b) fails without reasonable excuse to attend 3 consecutive meetings of the Commission;
- (c) has become bankrupt or has made an arrangement with his creditors;
- (d) is incapacitated by physical or mental illness;
- (e) engages in misbehaviour such as fraud, or has a conflict of interest as a result of engaging in paid employment that conflicts with the functions of the Commission; or
- (f) is otherwise unable or unfit to discharge the functions of a Commissioner.

Publication of names of Commissioners and changes of membership

9. The names of all of the Commissioners as first constituted and every change in the membership of the Commission shall be published in the *Official Gazette*.

Meetings

11.(1) The Commission shall meet at such times as may be necessary or expedient for the transaction of its business, and each meeting shall be held on such days and at such times and place as the Commission determines.

(2) Minutes of each meeting are to be kept by the Secretary or other person appointed by the Commission for the purpose, and are to be confirmed by the Commission at its next meeting and signed by the Chairman or other person presiding at that meeting.

Commission may regulate its own procedure

12. Subject to this *Schedule*, the Commission may regulate its own procedure and may delegate to any of its members the power and authority to carry out on behalf of the Commission such duties as the Commission determines.

Read three times and passed the House of Assembly this
day of _____, 2025.

Speaker

Read three times and passed the Senate this _____ day of
_____, 2025.

President