ST. CHRISTOPHER AND NEVIS

CHAPTER 16.06

INTERCEPTION OF COMMUNICATIONS ACT

Revised Edition
showing the law as at 31 December 2017

This is a revised edition of the law, prepared by the Law Commission under the authority of the Law Commission Act, Cap. 1.03.

This edition contains a consolidation of the following laws—

Printed under Authority by
The Regional Law Revision Centre Inc.
ANGUILLA

Published in
2019
Consolidated, Revised and Prepared under the Authority of the Law Commission Act,
on behalf of the Government of Saint Christopher and Nevis
by
The Regional Law Revision Centre Inc.,
P.O. Box 1626, 5 Mar Building,
The Valley, AI-2640, Anguilla,
West Indies.

Available for purchase from—

Attorney General's Chambers,
Government Headquarters, P.O. Box 164,
Church Street, Basseterre, St. Kitts,
West Indies

Tel: (869) 465-2521
Ext. 1013
Tel: (869) 465-2127
Fax: (869) 465-5040
Email: attorneygeneral@gov.kn

CHAPTER 16.06

INTERCEPTION OF COMMUNICATIONS ACT

ARRANGEMENT OF SECTIONS

PART V

DISCLOSURE AND ADMISSIBILITY OF INTERCEPTED COMMUNICATIONS

PART VI

LISTED EQUIPMENT

PART VII

TRIBUNAL

PART VIII

MISCELLANEOUS

CHAPTER 16.06

INTERCEPTION OF COMMUNICATIONS ACT

AN ACT TO PROVIDE FOR THE LEGAL FRAMEWORK FOR THE LAWFUL INTERCEPTION OF COMMUNICATIONS IN SAINT CHRISTOPHER AND NEVIS, AND FOR RELATED MATTERS.

PART I

PRELIMINARY MATTERS

Short title.

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

Interpretation.

2. (1) In this Act—

"authorised officer" means—

(a) the Commissioner of Police;

(b) the Director of the Financial Intelligence Unit;

(c) a person for the time being lawfully exercising the functions of a person stated in paragraph (a) or (b);

(d) a person authorised to act on behalf of a person mentioned in paragraph (a), (b) or (c);

(e) a person authorised to intercept communications under the Anti-Terrorism Act, Cap. 4.02, the Telecommunications Act, Cap. 16.05, the Electronic Crimes Act, Cap. 4.41 or any other law in Saint Christopher and Nevis;

"communication" includes—

(a) except in the definition "postal service", anything transmitted by means of a postal service, including a postal article; and

(b) anything comprising—

(i) speech, music, sounds, visual images or data of and description, including content data, computer data, traffic data, or electronic emissions thereof; or

(ii) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus,

conveyed across an electronic communication network or any part of the electronic network through the use of any electronic, mechanical, optical, wave, electromechanical, or other device;

(Substituted by Act 15 of 2012)

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

(Inserted by Act 15 of 2012)

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

(Inserted by Act 15 of 2012)

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

(Inserted by Act 15 of 2012)

"disclosure order" means an order made pursuant to section 21, requiring access to electronic data;

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

"intercept" means the acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the—

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examining, or inspection of the contents of any communication; and

(c) diversion of any communication from its intended destination to any other destination,

and "interception" shall be construed accordingly;

"intercepted communication" means any communication intercepted in the course of its transmission;

"interception device" means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus to intercept any communication but does not mean any instrument, device, equipment or apparatus, or any component thereof—

(a) furnished to the customer by a communications provider in the ordinary course of business and being used by the customer in the ordinary course of his or her business;

(b) furnished by such customer for connection to the facilities of such communications service and being used by the customer in the ordinary course of business; or

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

(Amended by Act 15 of 2012)

"interception direction" means a direction issued pursuant to sections 5 or 10;

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

(Inserted by Act 15 of 2012)

"judge" means a judge of the High Court;

"key" in relation to any electronic data, means any code, password, algorithm or other data the use of which, with or without keys—

(a) allows access to the data; or

(b) facilitates the putting of the data into an intelligible form;

"listed equipment" means any equipment declared to be listed equipment pursuant to section 26, and includes any component of such equipment;

"Minister" means the Minister responsible for national security;

"person" means a body corporate or an unincorporated body;

"postal provider" means any person who provides a postal service;

"postal service" means any service which—

(a) consists of the following, or one or more of them, namely the collection, sorting, conveyance, distribution and delivery whether in Saint Christopher and Nevis or elsewhere, of postal items; and

(b) is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to make available, or to facilitate, by means of transmission from place to place of postal items containing communications; or

(c) operates as a courier service,

and references to postal items shall be construed accordingly;

"protected information" means any electronic data, which, without a key, cannot, or cannot readily be accessed or put in an intelligible form;

"public postal service" means any postal service, which is offered or provided to, the public or to a substantial section of, the public in Saint Christopher and Nevis;

"terrorist activity" has the meaning given to it under the Anti-Terrorism Act, Cap. 4.02;

"Tribunal" means the Tribunal appointed pursuant to section 30.

(Definitions of "private telecommunications network", "public telecommunications network", "telecommunications provider", "telecommunications network and "telecommunications service" deleted by Act 15 of 2012)

(2) In this Act the interests of national security shall be construed as including, but not limited to, the protection of Saint Christopher and Nevis from threats of sabotage, espionage, terrorist activity, or subversion.

(3) For the purpose of this Act detecting an offence shall be taken to include—

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any offence may be committed; and

(b) the apprehension of the person by whom an offence was committed.

(4) Nothing in this Act shall be construed as requiring or prohibiting the anonymity or encryption of communications.

(Inserted as section 2A by Act 15 of 2012)

PART II

INTERCEPTION OF COMMUNICATIONS

Prohibition of interception.

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

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

(a) the communication is intercepted in accordance with an interception direction issued pursuant to section 5 or an entry warrant issued, pursuant to section 8, by a judge;

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

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

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

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

(f) the interception is of a communication transmitted by and received within an internal network which is used to serve the needs of a person using the network and is done by a person who has—

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

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

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

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

(b) an authorised officer believes that the interception of communication is necessary for the purpose of an emergency, of preventing death or injury or any damage to a person’s physical or mental health, or of mitigating any injury or damage to a person's physical or mental health or in the interests of national security.

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

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

(Amended by Act 15 of 2012)

Application for interception direction and unauthorised disclosure.

4. (1) An authorised officer who wishes to obtain an interception direction pursuant to the provisions of this Act, shall request the Director of Public Prosecutions to make an application *ex parte* to a judge in chambers on his or her behalf.

(2) Subject to section 10, an application referred to in subsection (1) shall be in writing in the prescribed form and shall be accompanied by an affidavit deposing the following—

(a) the name of the authorised officer on behalf of which the application is made;

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

(c) sufficient information for a judge to issue an interception direction on the terms set out in section 5(1);

(d) the ground referred to in section 5(1) on which the application is made;

(e) full particulars of all the facts and the circumstances alleged by the authorised person on whose behalf the application is made including—

(i) if practical, a description of the nature and location of the facilities from which, or the premises at which the communication is to be intercepted; and

(ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;

(f) if applicable, whether other investigative procedures have been applied and have failed to produce the required evidence or the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(g) the period for which the interception direction is required to be issued in accordance with section 7(5); and

(h) whether any previous application has been made for the issuing of an interception direction in respect of the same person, the same facility or the same premises specified in the application and, if such previous application exists, indicating the current status of that application and any other directives issued by the judge.

(3) Subsection 2(d) shall not apply in respect of an issue of an application of an interception direction on a ground referred to in section 5(1)(a), if a serious offence has been or is being or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime.

(4) Where an interception direction is applied for on the grounds of national security, the application shall be accompanied by a written authorisation signed by the Minister, authorising the application on that ground.

(5) Subject to subsection (6), the records relating to every application for an interception direction or the renewal or modification thereof shall be—

(a) placed in a packet and sealed by the judge to whom the application is made immediately on determination of the application; and

(b) kept in the custody of the court in a place to which the public has no access or such secure place as the judge may authorise.

(6) The records referred to in subsection (5), may be opened if a judge so orders only—

(a) for the purpose of dealing with an application for further authorisation; or

(b) for renewal of an authorisation,

unless otherwise ordered by the court.

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

(8) It shall be a defence in any proceedings against a person to show—

(a) that the disclosure was made by or to an attorney-at -law in connection with the giving, by the attorney-at-law to any client advice about the effect of the provisions of the Act; and

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

(9) It shall be a defence in proceedings against a person for an offence under subsection (7) to show that the disclosure was made by an attorney-at-law—

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

(b) for the purposes of the proceedings.

(10) Subsection (7) or subsection (8) shall not apply in the case of a disclosure made with a view to furthering any criminal purpose.

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

Issuance of interception direction.

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

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

(i) in the interests of national security; or

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

(iii) for the purpose, in circumstances appearing to the judge to be equivalent to those in which he or she would issue an interception direction by virtue of sub-paragraph (ii), of giving effect to the provisions of any mutual legal assistance agreement;

(b) other procedures—

(i) have not been or are unlikely to be successful in obtaining the information sought to be acquired by means of the interception direction;

(ii) are too dangerous to adopt in the circumstances; or

(iii) having regard to the urgency of the case are impracticable; and

(c) it would be in the best interests of the administration of justice to issue the interception direction.

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

Scope and form of interception direction.

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

(a) intercept, at any place in Saint Christopher and Nevis any communication in the course of its transmission;

(b) secure the interception in the course of its transmission by means of a postal service or communications network, or such communications as are described in the interception direction; and

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

(Amended by Act 15 of 2012)

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

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

(i) a particular person specified or described in the interception direction; or

(ii) a particular address specified or described in the interception direction; and

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

(Substituted by Act 15 of 2012)

(3) An interception direction shall specify the following—

(a) the identity of the—

(i) authorised officer on whose behalf the application is made pursuant to section 4, and the person who will execute the interception direction;

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

(iii) postal service provider or the communications provider to whom the interception direction to intercept must be addressed, if applicable.

(Amended by Act 15 of 2012)

(4) An interception direction may contain such ancillary provisions as are necessary to secure its implementation in accordance with the provisions of this Act or any other Act in Saint Christopher and Nevis.

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

(6) For the purposes of this section, "address" includes premises, postal address, e-mail address, internet protocol (IP) address, telephone number, or any number or designation used for the purposes of identifying communications networks, providers or apparatus.

(Inserted by Act 15 of 2012)

Duration of interception direction.

7. (1) An interception direction shall be valid for such period, not exceeding three months, as the judge may specify in the direction, provided that such direction may be renewed at any time before the end of that period upon application made pursuant to the provisions of subsections (3) and (4).

(2) A judge may, on an application for the renewal of an interception direction made by the Director of Public Prosecutions on behalf of an authorised officer, renew an interception direction at any time before the direction has expired.

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

(4) Every application for the renewal of an interception direction shall be made in the manner provided by section 4 and it shall be stated in the application—

(a) the reason and period for which the renewal is required; and

(b) the full particulars, together with times and dates, of any interceptions made or attempted under the direction, and an indication of the nature of the information that has been obtained by every such interception.

(5) Every application for the renewal of the interception warrant shall be supported by such other information as the judge may require.

(6) A renewal of an interception direction may be granted under this section if the judge is satisfied that the circumstances referred to in subsection (1) of section 5 still obtain.

(7) Every renewal of an interception direction shall be valid for such period, not exceeding ninety days, as the judge may specify in the renewal.

(8) If at any time before the end of the periods referred to in subsections (1) and (7), it appears to the authorised officer to whom the direction is issued, or a person acting on his or her behalf, that an interception direction is no longer necessary, he or she shall make an application to the judge for the revocation of the interception direction.

(Substituted by Act 15 of 2012)

Application, issuance, form, scope of entry warrant.

8. (1) An entry warrant shall not be issued by a judge, under this Act, unless there exists with respect to the premises to which the application for an entry warrant relates, a related interception direction.

(2) Where the Director of Public Prosecutions—

(a) makes an application for an interception direction on behalf of an authorised officer pursuant to section 4, the Director of Public Prosecutions may at the time of making the application, also apply to the judge for the issuance of an entry warrant; or

(b) makes an application on behalf of an authorised officer pursuant to section 4, the authorised person on whose behalf the application was made, or any other authorised officer may, at any such stage after the issuance of the interception direction in respect of which such an application was made, but before the expiry of the period or the extended period for which it has been issued, request the Director of Public Prosecutions to apply *ex parte* to a judge for the issuance of an entry warrant on his or her behalf.

(3) Subject to section 9, an application for an entry warrant referred to in subsection (2), shall be in writing and in the prescribed form and shall—

(a) be accompanied by an affidavit deposing the—

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

(ii) premises in respect of which the entry warrant is required; and

(iii) specific purpose for which the application is made;

(b) if the application is made in terms of subsection (2)(b), also contain, proof that an interception direction has been issued, and an affidavit setting forth the results, if any, obtained in the interception direction concerned, from the date of its issuance up to the date on which the application was made, or a reasonable explanation of the failure to obtain such results; and

(c) indicate whether any previous application has been made for the issuing of an entry warrant for the same purpose or in respect of the

same premises specified in the application and, if such previous application exists, indicate the status of the previous application.

(4) Subject to subsection (5), a judge may upon an application made to him by the Director of Public Prosecutions on behalf of an authorised officer, issue an entry warrant.

(5) An entry warrant shall be issued if the judge is satisfied, on the facts alleged in the application concerned that—

(a) the entry into the premises is necessary for the purpose—

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

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

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

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

(6) An entry warrant—

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

(b) shall contain the information referred to in subsection (3)(a)(ii) and (iii); and

(c) may contain conditions or restrictions relating to the entry upon the premises concerned as the judge may consider necessary.

(7) An entry warrant shall permit an authorised officer to enter upon the premises specified in the warrant for the purposes of—

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

(b) installing and maintaining an interception device; or

(c) removing an interception device.

(8) An entry warrant shall expire when—

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

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

(c) the interception direction to which it relates is terminated in accordance with sections 9 or 10,

whichever first occurs.

(9) When an entry warrant has expired pursuant to subsection (8)(a), the authorised officer on whose behalf the application was made or, if he or she is not available, any other authorised officer who would have been entitled to request the Director of Public Prosecutions to make the application, shall, as soon as practicable after the date of expiry of the entry warrant, and without applying to a judge for the issuing of a further entry warrant, remove, or cause to be removed, any interception device which has been installed and which, at the expiry date of the entry warrant, has not yet been removed from the premises concerned.

Termination of interception direction or entry warrant.

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

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

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

(ii) the judge, upon receipt of a report submitted pursuant to section 12 is satisfied that the objectives of the interception direction or the entry warrant or both, have been achieved; or

(iii) the grounds on which the interception direction or the purpose for which the entry warrant was issued, or both has ceased to exist; or

(iv) the conditions of the application referred to in subsection (1) of section 8 have changed in a way that an application would not be possible anymore; or

(Inserted by Act 15 of 2012)

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

(2) Where a judge terminates an interception direction or an entry warrant or both, pursuant to subsection (1), he or she shall forthwith, in writing, inform the authorised officer concerned of the termination.

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

(a) the contents of any communication intercepted under that direction 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; or

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

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

(5) Where an interception direction has been terminated pursuant to this section or section 10, an entry warrant issued pursuant to the interception direction shall also be deemed to be terminated.

Urgent application, etc.

10. (1) Where a judge is satisfied that the urgency of the circumstances so requires, the judge may dispense with the requirements for a written application and affidavit and proceed to hear an oral application made by the Director of Public

Prosecutions on behalf of an authorised officer for an interception direction, or an entry warrant, or both.

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

(a) contain the information referred to in subsection (6)(b) of section 8;

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

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

(3) A judge may, upon an oral application made to him or her, issue an interception direction or entry warrant, if he or she is satisfied that—

(a) there are reasonable grounds to believe that the interception direction or entry warrant or both should be issued; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, for the Director of Public Prosecutions to make a written application, on behalf of the authorised officer, for the issuing of the interception direction or entry warrant, applied for.

(4) Where the judge grants the application for an emergency interception direction or entry warrant, the judge shall forthwith make a note in writing of the particulars of the application, and shall also make a note of the terms of the interception direction or entry warrant.

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

(6) Where an interception direction or entry warrant or both is or are issued under this section, the Director of Public Prosecutions shall, on behalf of the authorised officer, within seventy-two hours of the time of issue, submit to the judge a written application and affidavit in accordance with the provisions of section 4(2) or 8(3), or both, as the case may be.

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

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

(9) If the judge is satisfied that the interception direction or entry warrant or both continues to be necessary, he or she shall make an order affirming the issue of the interception direction or entry warrant or both.

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

(11) Where an interception direction or entry warrant or both issued or renewed under this section is or are revoked under subsection (10), the direction or entry warrant or both, as the case may be, shall cease to have effect upon the revocation.

(12) Where the issue of an interception direction or entry warrant or both, is or are affirmed under subsection (9), the provisions of section 10 shall apply with respect to its duration as if the date of the order affirming the issue of the interception

direction or entry warrant were the date on which the interception direction or entry warrant was first given.

(Substituted by Act 15 of 2012)

Modification of interception direction and entry warrant.

11. A judge may modify any of the provisions of an interception direction or an entry warrant or both, at any time, after hearing representations from the Director of Public Prosecutions acting on behalf of an authorised officer and if he or she is satisfied that there is any change in the circumstances, which may make the requested modifications necessary or expedient.

Reports on progress.

12. A judge who has issued an interception direction or an entry warrant or both, 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 interception direction or the entry warrant or both, to report to him or her in writing—

(a) at such intervals as he or she determines on—

(i) the progress that has been made towards achieving the objectives of the interception direction or the entry warrant or both; and

(ii) any other matter which the judge deems necessary; or

(b) on the date of expiry of the entry warrant and interception direction concerned, or whether the interception device has been removed from the premises and, if so, the date of such removal.

Protection for acts done in good faith.

13. An authorised officer shall not be liable for any acts done by him or her in good faith pursuant to the provisions of this Act.

PART III

EXECUTION OF INTERCEPTION DIRECTIONS AND ENTRY WARRANTS

Execution of interception direction or entry warrant.

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

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

(3) Where a postal article has been taken possession of pursuant to subsection (2), the authorised officer who executes the interception direction and the entry warrant or assists with the execution thereof—

(a) shall take proper care of the postal article and may, if the postal article concerned is perishable, with due regard to the interests of the persons concerned, dispose of that postal article in such manner as circumstances may require;

(b) shall return the postal article, if it has not been disposed of in terms of paragraph (a), or cause it to be returned to the postal provider if, in the opinion of the authorised officer concerned—

(i) no criminal or civil proceedings as contemplated will be instituted in connection with the postal article or;

(ii) the postal article will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes of an order of the court; and

(iii) such postal article may be returned without prejudice to the national security of Saint Christopher and Nevis, as the case may be.

Entry on premises for execution of entry warrant.

15. If an entry warrant has been issued pursuant to the provisions of this Act, an authorised officer who executes or assists with the execution thereof, may at any time during which the entry warrant is in force, without prior notice to the owner or occupier of the premises specified in the entry warrant, enter the said premises and perform any act relating to the purpose for which the entry warrant has been issued.

Duty to provide assistance.

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

(2) Where an authorised officer intends to seek the assistance of any person in executing an interception direction or an entry warrant or both, a judge shall, on the request of the Director of Public Prosecutions, appearing on behalf of the authorised officer, direct appropriate persons to furnish information, facilities, or technical assistance as may be necessary to accomplish the interception.

(3) A person who knowingly fails to comply with his or her duty under subsection (2) commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding one year.

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

(5) Any person directed to provide assistance by way of information, facilities, or technical assistance pursuant to subsection (2), shall promptly comply in such a manner that the assistance is rendered—

(a) as unobtrusively as possible; and

(b) with the minimum interference to the services that such a person or entity normally provides to the party affected by the interception direction or entry warrant, as can reasonably be expected in the circumstances.

(6) For the purposes of this Act, the provision of assistance includes any disclosure of intercepted material and related communication data to an authorised officer.

Confidentiality of intercepted communications.

17. (1) Where a judge issues an interception direction or an entry warrant, he or she shall issue such an interception direction or an entry warrant or impose such terms or conditions in the interception direction or entry warrant as he or she 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 part of the communication,

is limited to the minimum that is necessary for the purposes for which the interception direction or entry warrant or both, was issued or for any prosecution for an offence; and—

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

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

(ii) destroyed as soon as retention is no longer necessary.

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

(3) A person who fails to comply with subsection (2) commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars.

Conduct of authorised officer on premises.

18. An authorised officer who has entered premises, pursuant to section 15, shall act in accordance with the provisions of the Code of Conduct referred to in section 37.

Assault of authorised officer.

19. A person who assaults an authorised officer, who enters premises pursuant to section 15, shall be liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment.

Offence of unauthorised disclosure of interception.

20. (1) Where an interception direction or an entry warrant or both, has been issued or renewed, every person mentioned under subsection (2) shall keep the following information confidential—

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

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

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

(d) the steps taken pursuant to the interception direction or the entry warrant or of any such requirement; and

(e) everything in the intercepted material together with any related communications data.

(2) The persons referred to in subsection (1), are—

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

(b) any person holding office under the State;

(c) any person employed by or for the purpose of the Police Force or the Financial Intelligence Unit;

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

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

(3) A person, referred to in subsection (2), who makes a disclosure to any person of anything that he or she is required to keep confidential under subsection (1) commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding one year, or to both such fine and imprisonment.

(4) It shall be a defence in any proceedings against a person pursuant to subsection (3) to show—

(a) that the disclosure was made by or to an attorney-at -law in connection with the giving, by the attorney-at-law to any client advice about the effect of the provisions of the Act; and

(b) the person to whom, or as the case may be, by whom a disclosure referred to in subsection (3) was made, was the client or a representative of the client.

(5) It shall be a defence in proceedings against a person for an offence under subsection (3) to show that the disclosure was made by an attorney-at-law—

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

(b) for the purposes of the proceedings.

(6) Subsection (4) or subsection (5) shall not apply in the case of a disclosure made with a view to furthering any criminal purpose.

(7) In proceedings against a person for an offence under subsection (3), it shall be a defence for the person to show that the disclosure was confined to a disclosure permitted by the authorised officer.

(8) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was confined to a disclosure authorised—

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

(b) by the terms of the requirements to provide assistance pursuant to section 16; or

(c) by section 16(6).

PART IV

PROTECTED INFORMATION

Order requiring disclosure of protected information.

21. (1) Where protected information has come into the possession of an authorised officer by virtue of an interception direction or an entry warrant or both, pursuant to this Act, or by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so, or has otherwise come into the possession of an authorised officer by any other lawful means, and he or she has reasonable grounds to believe that—

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

(b) disclosure of the information is necessary for any of the purposes specified in section 5(l)(a)(i) or (ii),

the Director of Public Prosecutions may apply in the prescribed form on his or her behalf to a judge in chambers for a disclosure order requiring the person whom he believes to have possession of the key to provide disclosure in respect of the protected information.

(2) A disclosure order under subsection (1)—

(a) shall—

(i) be in writing in the prescribed form;

(ii) describe the protected information to which the order relates;

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

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

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

(3) A disclosure order granted pursuant to this section shall not require the disclosure of any key which—

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

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

(4) In granting a disclosure order required for the purposes of subsections (1) and (2), the judge shall take into account—

(a) the extent and the nature of any other protected information outside the scope of the order to which the key is also a key; and

(b) any adverse effect that complying with the order might have on a business carried on by a person to whom the order is addressed,

and shall permit such disclosure as is proportionate to what is sought to be achieved, allowing, where appropriate, for disclosure in such a manner as would result in the putting of the information in an intelligible form other than by disclosure of the key itself.

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

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

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

Effects of disclosure order.

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

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

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

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

(a) he or she makes, instead, a disclosure of any key to the protected information that is in his or her possession; or

(b) the disclosure is made in accordance with the order, with respect to the person to whom, and the time in which, the person to whom the disclosure order was addressed was required to disclose the information.

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

(a) not in possession of the protected information to which the order relates; or

(b) incapable, without the use of a key that is not in his or her possession, of obtaining access to the protected information or disclosing it in an intelligible form,

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

(4) It shall be sufficient for the purposes of complying with a disclosure order for the person to whom it is addressed to disclose only those keys, the disclosure of which is sufficient to enable the person to whom they are disclosed to obtain access to the protected information and to put it in an intelligible form.

(5) Where—

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

(b) there are different keys, or a combination of keys, in the possession of the person referred to in paragraph (a), the disclosure of which would constitute compliance with the order,

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

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

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

(b) if he or she had continued to have the key to the protected information in his or her 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 to the protected information or the putting of the protected information into an intelligible form,

that person shall disclose to the person to whom he or she is required to disclose the key, all such information as is mentioned in paragraph (c) for the purpose therein mentioned.

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

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

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

(b) every key disclosed pursuant to the disclosure order is stored, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the information or put it in an intelligible form; and

(c) the number of—

(i) persons to whom the key is disclosed or otherwise made available; and

(ii) copies made of the key,

is limited to the minimum that is necessary for the purpose of enabling the protected information to be accessed or put into an intelligible form.

(9) Subject to subsection (10) where any relevant person incurs any loss or damage as a consequence of—

(a) any breach by a person of the duty imposed upon him or her by subsection (8); or

(b) any contravention by any person of arrangements made pursuant to subsection (10) in relation to persons under the control of a person to whom subsection (8) applies,

the breach or contravention shall be actionable against that person at the suit or instance of the relevant person in accordance with section 30 (3).

(10) A person is a relevant person for the purposes of subsection (9) if he or she is—

(a) a person who has made a disclosure in pursuance of an order made under section 18; or

(b) a person whose protected information or key has been disclosed in pursuance of an order made under section 18,

and loss or damage shall be taken into account for the purposes of section 18 to the extent only that it relates to the disclosure of a particular protected information or a particular key which, in the case of a person falling within paragraph (b), shall be his or her information or key.

(11) For the purposes of subsection (10)—

(a) information belongs to a person if he or she has any right that would be infringed by an unauthorised disclosure of the information; and

(b) a key belongs to a person if it is a key to information that belongs to him or her or he or she has any right that would be infringed by an unauthorised disclosure of the key.

Tipping-off.

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

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

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

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

(2) A disclosure order made under section 21 shall not contain a requirement to keep anything secret except where the protected information to which it relates has come, or is likely to come, into possession of an authorised officer by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of safety or well-being of any person, to keep confidential from a particular person.

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

(4) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that—

(a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and

(b) the person could not reasonably have been expected to take steps, after the disclosure order was issued to him or her or, as the case may be, on becoming aware of it or of its contents, to prevent the disclosure.

(5) It shall be a defence in any proceedings against a person to show—

(a) that the disclosure was made by or to an attorney-at-law in connection with the giving, by the attorney-at-law to any client advice about the effect of the provisions of the Act; and

(b) the person to whom, or as the case may be, by whom a disclosure was made, was the client or a representative of the client.

(6) It shall be a defence in proceedings against a person for an offence under this section to show that the disclosure was made by an attorney-at-law—

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

(b) for the purposes of the proceedings.

(7) Subsection (5) or subsection (6) shall not apply in the case of a disclosure made with a view to furthering any criminal purpose.

(8) In proceedings against any person for an offence under this section it shall be a defence for that person to show that the disclosure was authorised—

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

(b) by or on behalf of a person who—

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

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

(9) In proceedings for an offence under this section against a person other than the person to whom the disclosure order under section 21 was addressed, it shall be a defence for the person against whom the proceedings are brought to show that he or she neither knew nor had reasonable grounds for suspecting that the order contained a requirement to keep confidential what was disclosed.

PART V

DISCLOSURE AND ADMISSIBILITY OF INTERCEPTED COMMUNICATIONS

Disclosure of communications data.

24. (1) For the purposes of this section—

"communications data" means any—

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

(b) information, that does not include the contents of a communication, other than data falling within paragraph (a) which is about the use, made by any person—

(i) of any postal service or 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; and

(c) information not falling within paragraph (a) or paragraph (b) that is held or obtained, in relation to persons to whom he or she provides the service, by a person providing a postal or a telecommunications service;

"designated person" means the Minister or any person prescribed for the purposes of this section by the Minister by order published in the *Gazette* and subject to negative resolution of the National Assembly;

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

(a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;

(b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted;

(c) comprising signals for the actuation of—

(i) apparatus used for the purposes of a telecommunications network for effecting, in whole or in part, the transmission of any communications; 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 a computer programme, access to which is obtained or which is run by means of the communication, to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.

(2) Where it appears to the court that a person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the court may, by order, require the provider—

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

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

(3) The court shall not issue an order under subsection (2) in relation to any communications data unless it is satisfied that it is necessary to obtain the data and to disclose the data to an authorised person.

(4) The court shall not issue an order under subsection (2) in relation to any communications data unless it is satisfied that it is necessary to obtain that data—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing public disorder;

(c) in the interests of the economic well-being of Saint Christopher and Nevis;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose in an emergency, of preventing death, injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) for any purpose, not falling in paragraphs (a) to (g) which are specified for the purposes of this section by an order published in the *Gazette* made by the Minister pursuant to this section.

(5) An order made pursuant to this section shall state—

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

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

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

(d) the matters falling within subsections (3) and (4) by reference to which the order is issued; and

(e) the date on which it is issued.

(6) An order, issued pursuant to this section, shall not require—

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

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

(7) The provisions of sections 21 and 22, relating to disclosure orders, shall apply in relation to the disclosure of data pursuant to an order made in accordance with this section.

(8) Subject to subsection (9), a provider of a telecommunications service, to whom an order is issued under this section, shall not disclose to any person the existence or operation of the order, or any information from which such existence or operation could reasonably be inferred.

(9) The disclosure referred to in subsection (8) may be made to—

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

(b) an attorney-at-law for the purpose of providing legal advice or representation in relation to the order.

(10) A person referred to in paragraph (a) or (b), of subsection (9), shall not disclose the existence or operation of the order, except to the authorised officer specified in the order for the purpose of—

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

(b) giving legal advice or making representations in relation to the order, in the case of an attorney-at-law.

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

(a) as permitted by the order;

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

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

(12) A person who contravenes subsection (8), (9), (10) or (11) commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding one year or to both such fine and imprisonment.

Admissibility of evidence.

25. (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 that might result in the disclosure of any of the details pertaining to the method by which data was obtained;

(b) the identity of any party who supplied the data; or

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

(2) Subject to section 9(3), the contents of a communication that is obtained in accordance with an interception direction issued under section 5 shall be admissible as evidence in any criminal proceedings or civil proceedings in accordance with the law relating to the admissibility of evidence.

(3) In any criminal proceedings or civil 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 or section 10, 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 proceedings in respect of an offence under this Act, including any proceedings before the Tribunal referred to in section 30 in relation to an offence committed in contravention of the provisions of this Act, but if the court is satisfied that—

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

(b) the parties to the proceedings would not he unduly prejudiced thereby, the court may exclude such disclosure.

PART VI

LISTED EQUIPMENT

Listed equipment.

26. (1) The Minister may, by notice published in the *Gazette*, declare any electronic, electro magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the notice, to be listed equipment.

(2) A notice under subsection (1) may at any time be amended or revoked.

(3) Before the Minister exercises the powers conferred upon him or her under subsection (1), he or she shall cause to be published in the *Gazette* a draft of the proposed notice, together with a notice inviting all interested parties to submit to him or her in writing and within a specified period, comments and representations in connection with the proposed notice.

(4) A period not less than one month shall elapse between the production of the draft notice and the publication of the notice under subsection (1).

(5) Subsection (3) shall not apply—

(a) if the Minister, in pursuance of comments and representations received in terms of subsection (3) decides to publish a notice referred to in subsection (1) in an amended form;

(b) to any notice in terms of subsection (1) in respect of which the Minister is of the opinion that the public interest requires that it be made without delay.

(6) Any notice under subsection (1) shall be subject to negative resolution of the National Assembly.

Prohibition on manufacture and possession of listed equipment.

27. (1) Subject to subsection (2) of this section and section 28, a person shall not manufacture, assemble, possess, sell, or purchase any listed equipment.

(2) Subsection (1) shall not apply to any authorised officer or any other person who manufactures, assembles, possesses, sells, purchases, or advertises listed equipment under the authority of a certificate of exemption issued to him or her by the Minister under section 28.

Exemptions.

28. (1) The Minister may, upon application made by a person in the prescribed form, and acting upon the advice of Cabinet, exempt a person from one or all of the prohibited acts listed under subsection (1) of section 27 for such period and on such terms as the Minister may determine.

(2) The Minister shall grant an exemption under subsection (1) if he or she is satisfied that—

(a) the exemption is in the public interest; or

(b) special circumstances exist which justify the exemption.

(3) An exemption under subsection (1) shall be granted by issuing to the person concerned, a certificate of exemption, in the prescribed form in which his or her name, and the scope, period and conditions of the exemption are specified.

(4) A certificate of exemption granted under subsection (3) shall be published in the *Gazette* and shall become valid upon the date of such publication.

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

(6) A certificate of exemption lapses upon—

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

(b) withdrawal under subsection (5).

Offence of contravention of section 27.

29. (1) A person who contravenes or fails to comply with section 27 commits an offence and shall be liable on summary conviction to a fine not exceeding twenty five thousand dollars or, to a term of imprisonment not exceeding five years or to both such fine and imprisonment.

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

(a) by means of which the offence was committed;

(b) which was used in connection with the commission of the offence;

(c) which was found in the possession of the convicted person; or

(d) the possession of which constituted the offence,

to be forfeited to the State.

(3) Where a person is convicted of an offence referred to in subsection (1), the court shall, in addition to the penalty which it may impose in respect of the offence, declare forfeited to the State any equipment other than listed equipment which was found in the possession of the convicted person and—

(a) the possession of which constitutes an offence;

(b) by means of which the offence was committed; or

(c) which was used in connection with the commission of the offence.

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

(5) Any listed equipment or other equipment delivered to the Commissioner of Police pursuant to subsection (4) shall, in the case of—

(a) listed equipment declared forfeited under subsection (2), be kept by the Commissioner of Police—

(i) for a period not less than four months with effect from the date of declaration of forfeiture; or

(ii) if an application under subsection (8) is made, for a period not exceeding 30 days with effect from the date of the final decision in respect of the application;

(b) equipment declared forfeited under subsection (3), be kept by the Commissioner of Police—

(i) for a period not less than four months with effect from the date of declaration of forfeiture; and

(ii) if an application under subsection (8) is made, for a period not exceeding thirty days with effect from the date of the final decision in respect of the application,

subject to subsections (8) and (9) be destroyed by the Commissioner of Police.

(6) The Commissioner of Police shall as soon as practicable after the expiry of the period referred to in—

(a) paragraph (a) (i) or (b) (i) of subsection (5); or

(b) paragraph (a) (ii) or (b) (ii) of subsection (5) if an application referred to has been refused,

destroy such listed equipment in his or her possession.

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

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

(b) he or she has taken all reasonable steps to prevent the use of the listed equipment in connection with an offence; and

(c) could not reasonably be expected to have known or had no reason to suspect that the listed equipment concerned was being or would be used in connection with the offence.

(8) A judge may, upon an application made at any time within a period not exceeding three months with effect from the date of declaration of forfeiture under subsection (2) or (3), by any person other than the convicted person, who claims that—

(a) the listed equipment or the equipment referred to in subsection (2) or (3) is his or her property; and

(b) he or she is a person referred to in subsection (9),

inquire into and determine those matters.

(9) If the judge under subsection (8) is satisfied that the—

(a) listed equipment or other equipment concerned is the property of the person;

(b) the person concerned is a person referred to in subsection (8); and

(c) the person was not directly connected with the commission of the offence,

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

PART VII

TRIBUNAL

Establishment of Tribunal.

30. (1) There shall be established, for the purpose of exercising jurisdiction conferred upon it by this section, a Tribunal consisting of a judge who shall be appointed by the Governor-General acting on his or her own deliberate judgement.

(2) The Tribunal shall—

(a) be the only forum for the purposes of any proceedings under any law of Saint Christopher and Nevis which shall fall within subsection (3) of this section;

(b) consider and determine any complaints made to the Tribunal which, in accordance with subsection (4), are complaints for which the Tribunal is the appropriate forum.

(3) Proceedings fall within this subsection if—

(a) they are proceedings brought by virtue of section 22(9); or

(b) they are proceedings relating to the taking place in any challengeable circumstances of any conduct falling within subsection (5).

(4) The Tribunal shall be the appropriate forum for any complaint if it is a complaint by a person who is aggrieved by any conduct falling within subsection (5), which he or she believes—

(a) to have taken place in relation to him or her, to any communications sent by him or her, or intended for him or her, or to his or her use of any postal service, telecommunications service or telecommunications network; and

(b) to have taken place in challengeable circumstances.

(5) Conduct shall fall within this subsection if it is—

(a) conduct for or in connection with the interception of communications in the course of its transmission by means of a postal service or a telecommunications service;

(b) any disclosure or use of a key to protected information.

(6) For the purposes of this section conduct takes place in challengeable circumstances if—

(a) it is conduct by or on behalf of a person holding any office, rank or position in the Police Force or the Financial Intelligence Unit, or any other position under the State; and

(b) the conduct took place without the authority of an interception direction or an entry warrant, or otherwise without authority under this Act.

(7) Without prejudice to subsection (6), conduct does not take place in challengeable circumstances to the extent that it is authorised by, or takes place with the permission of a judicial authority.

(8) In subsection (7) "judicial authority" means a Judge or a magistrate.

Exercise of Tribunal's jurisdiction.

31. (1) The Tribunal shall not be under any duty to hear, consider or determine any proceedings, complaint or reference if it appears to it that the bringing of the proceedings or the making of the complaint or reference is frivolous or vexatious.

(2) Except where the Tribunal, having regard to all the circumstances, is satisfied that it is equitable to do so, it shall not consider any complaint made by virtue of section 30(2)(b) if it is made more than one year after the taking place of the conduct to which it relates.

(3) Subject to any provision made by the rules pursuant to section 33, where any proceedings have been brought before the Tribunal or any reference made to the Tribunal, it shall have power to make such interim orders, pending its final determination, as it thinks fit.

(4) Subject to any provision made by rules referred to in section 33, the Tribunal on determining any proceedings, complaint or reference shall have the power to make any award of compensation or other order as it thinks fit, including an order requiring the destruction of any records of information, which is held by any public authority in relation to any person.

(5) All determinations, awards, orders and other decisions of the Tribunal, shall be binding and final.

Tribunal procedure

32. (1) Subject to any rules made pursuant to section 33 the Tribunal shall be entitled to determine its own procedure in relation to any proceedings, complaint or reference brought before or made to it.

(2) In determining its procedure under this section, the Tribunal shall have regard in particular to—

(a) the need to ensure that matters which are the subject of proceedings, complaints or references brought before or made to the Tribunal are properly heard and considered; and

(b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security or the prevention or detection of serious crime, and without prejudice to the generality of the foregoing, may in particular follow any procedure mentioned in section 33(4) for that purpose.

(3) Where the Tribunal determines any proceedings, complaint or reference brought before or made to it, it shall give—

(a) a statement that the Tribunal has made a determination that is in the complainant's favour; or

(b) a statement that the Tribunal has made a determination that is not in the complainant's favour.

Tribunal rules.

33. (1) The Minister may make rules regulating—

(a) the exercise by the Tribunal of the jurisdiction conferred on it by section 30(2);

(b) any matters preliminary or incidental to, or arising out of, the hearing or consideration of any proceedings, complaint or reference brought before or made to the Tribunal.

(2) Without prejudice to the generality of subsection (1), rules under this section may—

(a) specify the forms of hearing or consideration to be adopted by the Tribunal in relation to particular proceedings, complaints or references, including where applicable, the mode and burden of proof and the admissibility of evidence;

(b) require information about any determination, award, order or other decision made by the Tribunal in relation to any proceedings, complaint or reference to be provided, in addition to any statement under section 32(3) to the person who brought the proceedings or made the complaint or reference to the person representing his or her interests.

(3) Rules made pursuant to this section may provide—

(a) for a person who has brought any proceedings before or made any complaint or reference to the Tribunal to have the right to be legally represented;

(b) for the manner in which the interests of a person who has brought any proceedings before or made any complaint or reference to the Tribunal are otherwise to be represented;

(c) for the appointment in accordance with the rules, by such person as may be determined by the rules, of a person to represent those interests in the case of any proceedings, complaint or reference.

(4) Rules made pursuant to this section may in particular enable or require the Tribunal to proceed in the absence of any person, including the person making the complaint or reference and any legal representative of the person, and to exercise its jurisdiction, and to exercise and perform its powers and duties, including in particular, in relation to the giving of reasons, in such a manner provided for in the rules as prevents or limits the disclosure of particular matters.

(5) Rules made pursuant to this section may provide for the application, with or without modification, of the provisions contained in specified rules of court.

(6) All rules made under this section shall be subject to negative resolution of the National Assembly.

PART VIII

MISCELLANEOUS

Amendment of Schedule.

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

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

False statements.

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

Regulations.

36. (1) The Minister may make Regulations prescribing any matter or thing in respect of which it may be expedient to make Regulations for the purpose of carrying this Act into effect.

(2) Without prejudice to the generality of the foregoing, the Minister may make Regulations particularly to prescribe the forms required by this Act.

Code of Conduct.

37. The Minister may prescribe a Code of Conduct for authorised officers.

Annual Report.

38. (1) The Minister shall, as soon as possible 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 interception directions and entry warrants applied for to intercept communications;

(b) the number of interception directions and entry warrants granted by the Court;

(c) the number of interception directions and entry warrants applied for and granted under section 10;

(d) the average period for which interception directions and entry warrants were granted;

(e) the number of interception directions and entry warrants refused by the Court;

(f) the number of applications made for renewals;

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

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

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

(j) the number of criminal proceedings commenced by the State in which private communications obtained by interception under an interception direction 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 an interception direction 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 as a result of an interception under an interception direction 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 under subsection (1) to be laid before the National Assembly promptly after its completion.

Allocation of costs.

39. (1) Subject to subsection (2), any costs incurred by a communications provider which enable the communications provider to intercept communications or store communications, including the investment, technical, maintenance and operating costs shall be borne by that communications provider.

(2) The Minister may, by regulations, establish a system of reimbursement of direct costs incurred by a communications provider in respect of personnel and administration which are required for the purposes of providing assistance in execution of interception directions.

(Inserted by Act 15 of 2012)

———————

SCHEDULE

(Section 5(1) and Section 34)

1. Murder
2. Manslaughter
3. Treason
4. Kidnapping
5. Abduction
6. Robbery
7. Blackmail
8. Fraud
9. Hijacking
10. Extortion
11. Counterfeiting
12. Corruption
13. Arson
14. An offence contrary to the provisions of the Proceeds of Crime Act, Cap. 4.28 and the Anti-Money Laundering Regulations.
15. An offence contrary to the provisions of the Drugs (Prevention and Abatement of the Misuse and Abuse of Drugs) Act, Cap. 9.08.
16. An offence contrary to the provisions of the Firearms Act, Cap. 19.05.
17. An offence contrary to the provisions of the Anti-Terrorism Act, Cap. 4.02.
18. Attempting or conspiring to commit or aiding, abetting, counseling or procuring the commission of, an offence falling within any of the preceding paragraphs.

———