THE INTERCEPTION OF COMMUNICATIONS ACT

ARRANGEMENT OF SECTIONS

1. Short title.
2. Interpretation.
3. Prohibition of interception.
4. Warrant for interception.
5. Scope of warrant.
6. Duration of warrant.
7. Application for warrant in urgent circumstances.
8. Modification of warrants.
9. Protection of authorized officer.
10. Duties of persons providing assistance or telecommunications services.
11. Confidentiality of intercepted communication.
12. Order requiring disclosure of protected communication.
13. Effect of disclosure order.
14. Admissibility of evidence.
15. Offences.
16. Disclosure of communications data.
17. Admissibility of communications data.
18. Amendment of Schedule.
19. Regulations.

SCHEDULE

[The inclusion of this page is authorized by L.N. 11/2010]

THE INTERCEPTION OF COMMUNICATIONS ACT

[*15th March, 2002.*]

Acts 5 of 2002, 18 of 2005 2nd Sch., 17 of 2006, 12 of 2009 3rd Sch. 3 of 2010 S. 22., 21 0f 2011, 26 of 2013 2nd Sch., 39 of 2013 S. 39(4).

Short title.

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

Interpretation.

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

"authorized officer" means—

(*a*) the Commissioner of Police;

(*b*) the officer of the Jamaica Constabulary Force in charge of—

(i) internal security; or

(ii) the National Firearm and Drug Intelligence Centre or any organization replacing the same; or

(*c*) the Chief of Staff, or the head of the Military Intelligence Unit, of the Jamaica Defence Force;

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

"electronic signature" means anything in electronic form which—

(*a*) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

(*b*) is generated by the signatory or other source of the communication or data; and

(*c*) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

"intercept" in relation to a communication means the—

(*a*) monitoring of transmissions made by wireless telegraphy to or from apparatus comprising in the network;

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

"Judge" means a Judge of the Supreme Court;

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

(*a*) allows access to a protected communication; or

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

"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 Jamaica 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 Jamaica;

(*b*) anywhere outside of Jamaica,

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

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

(*a*) in the form of—

(i) speech, music or other sounds;

(ii) visual images, whether still or animated;

(iii) data or text;

(iv) any type of signals;

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

(*c*) in any combination of forms; and

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

"telecommunications network" means a system of telecommunications or any part thereof whereby a person or thing can send or receive intelligence to or from any point in Jamaica;

"telecommunications service" means a service provided by means of a telecommunications network to any person for the transmission of intelligence from, to or within Jamaica without change in the content or form;

18/2005
2nd Sch.

"terrorism offence" has the meaning assigned to it by section 2 of the Terrorism Prevention Act.

(2) In this Act, the interests of national security shall be construed as including, but not limited to, the protection of Jamaica from threats of espionage, sabotage, any terrorism offence or subversion. 18/2005 2nd Sch.

3.—(1) Except as provided in this section, a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunications network commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to imprisonment for a term not exceeding three years or to a fine not exceeding three million dollars or to both such fine and imprisonment. Prohibition of interception.

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

(*a*) the communication is intercepted in obedience to a warrant issued by a Judge under section 4;

(*b*) he 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 intercepted as an ordinary incident to the provision of telecommunications services or to the enforcement of any enactment relating to the use of those services;

(*d*) the communication is not a private communication;

(*e*) the communication is a stored communication and is acquired in accordance with the provisions of any other law; or

(*f*) the interception is of a communication transmitted by a network that is not a public 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 sub-paragraph (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 purposes 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.

Warrant for interception.

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

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

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

21/2011 S. 2(a).

(1A) For the purposes of subsection (1)(*b*), a warrant may authorize that the intercepted communication be disclosed, by a person referred to in subsection (1)(*b*), to a foreign government, or any agency of such government—

(*a*) where there exists between Jamaica and such foreign government an agreement for the mutual exchange of that kind of information and the Minister certifies that it is in the public interest that such disclosure be made;

(*b*) if the Judge is satisfied that the foreign government, or any agency of such government, to whom the communication is to be disclosed undertakes to—

(i) keep the information confidential in accordance with arrangements made pursuant to directions issued under section 11; and

(ii) use the communication solely for the purpose of the prevention, detection or prosecution of a criminal offence; and

(*c*) subject to such other conditions as the Judge thinks it appropriate to impose with a view to ensuring the matters referred to in section 11(1)(*a*) and (*b*);

(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 specified 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; 39/2013 S. 39(4).

(*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 attaining 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; and

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

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

(*a*) an affidavit deposing to the following matters—

(i) the name of the 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 5;

(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 5(3);

(*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; and

(*c*) where disclosure to a foreign government, or any agency of such government, is contemplated pursuant to subsection (1A), the certification of the Minister that it is in the public interest that such disclosure be made. 21/2011 S. 2 (b)(iii).

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

(5) A person who discloses the existence of a warrant or an application for a warrant, other than to a person to whom such disclosure is authorized for the purposes of this Act, commits an offence and shall be liable upon summary conviction before a Resident Magistrate to a fine not exceeding three million dollars or to imprisonment for a term not exceeding three years, or to both such fine and imprisonment.

Scope of warrant.

5.—(1) A warrant shall authorize the interception of—

(*a*) communication transmitted by means of a public or private telecommunications network to or from—

17/2006 S. 2(a).

(i) any person specified or described in the warrant; or

(ii) any premises so specified or described; and

17/2006 S. 2(b).

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

(2) A warrant shall specify—

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

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

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

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

(*e*) the period for which it is valid.

17/2006 S. 2(c).

(2A) The provisions of a warrant describing the types of communications sought to be intercepted shall—

(*a*) be comprised in one or more schedules to the warrant, setting out the address, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications sought to be intercepted; and

(*b*) authorize to be included in any of those schedules any other such addresses, numbers, apparatus or other factors, or combination of factors, that an authorized officer may specify by instrument in writing issued by him.

(2B) Any factor or combination of factors set out in accordance with subsection (2A) shall be such as identifies communications that are likely to be or to include— 17/2006 S. 2(c).

(*a*) communications from, or intended for, the person specified or described in the warrant; or

(*b*) communications originating on, or intended for transmission to, the premises so specified or described.

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

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

(5) In this section— 17/2006 S. 2(d).

"address" includes a location, e-mail address, telephone number or other number or designation used for the purpose of identifying telecommunications networks or apparatus;

"person" includes an organization and any association or combination of persons.

Duration of warrant.

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

(2) A Judge may—

(*a*) on an application by an authorized 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 ninety days from the date of expiration of the initial period.

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

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

Application for warrant in urgent circumstances.

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

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

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

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

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

(*a*) make an order revoking the warrant if—

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

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

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

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

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

Modification of warrants. 17/2006 S. 3.

8.—(1) A Judge may modify a warrant—

(*a*) at any time, after hearing representations from an authorized officer and if satisfied that there is any change in—

(i) the circumstances that constituted grounds for the issue or renewal of the warrant; or

(ii) any of the identifying factors referred to in section 5(2A); or

(*b*) upon the application of an authorized officer under subsection (2), by including any of the factors specified in an instrument issued pursuant to section 5(2A)(*b*).

(2) An authorized officer who issues an instrument in writing pursuant to section 5(2A)(*b*) shall, within the time specified in subsection (3), apply to a Judge for a modification of the warrant to include the factors specified in the instrument.

(3) An application under subsection (2) shall be made as soon as is reasonably practicable, but in any event within the period of seven days (exclusive of Saturdays, Sundays and public general holidays) next following the date of the issue of the instrument.

(4) An instrument in writing issued pursuant to section 5(2A)(*b*) shall—

(*a*) be valid as from the date of its issue;

(*b*) cease to be valid at the end of the period referred to in subsection (3), or such earlier time as the Judge who considers the application for modification shall specify; and

(*c*) for the period of its validity, be deemed to be a scheduled part of the warrant.

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

Protection of authorized officer.

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

Duties of persons providing assistance or telecommunications services.

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

(*a*) as unobtrusively; and

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

as can reasonably be expected in the circumstances.

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

(4) Subject to subsection (5), the cost of complying with the provisions of— 17/2006 S. 4.

(*a*) subsection (1) shall be borne by the person providing the telecommunications service; and

(*b*) subsection (2) shall be borne by the person or entity directed to provide the assistance.

17/2006
S. 4.

(5) The Minister may make regulations—

(*a*) prescribing, in accordance with recognized international standards, minimum requirements for securing compliance with subsection (1); and

(*b*) determining the manner in which the reasonable costs of complying with subsection (1) or (2) may be—

(i) apportioned; and

(ii) recovered by the persons referred to in subsection (4).

Confidentiality of intercepted communication.

11.—(1) Where a Judge issues a warrant, he shall issue such directions as he considers appropriate for the purpose of requiring the authorized officer to make such arrangements as are necessary—

(*a*) for ensuring that—

(i) the extent to which the intercepted communication is disclosed;

(ii) the number of persons to whom any of that communication is disclosed;

(iii) the extent to which any such communication is copied; and

(iv) the number of copies made of any of the communication,

is limited to the minimum that is necessary for the purposes of the investigations in relation to which the warrant was issued or of any prosecution for an offence; and

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

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

(ii) destroyed as soon as its retention is no longer necessary for those purposes.

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

Order requiring disclosure of protected communication.

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

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

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

the officer may apply to a Judge in Chambers for 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, being a reasonable time in all the circumstances; and

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

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

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

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

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

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

(*a*) the extent and nature of any protected communication, in addition to the intercepted communication, to which the key is also a key; and

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

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

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

(*a*) the authorized officer; or

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

Effect of disclosure order.

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

(*a*) shall be entitled to use any key in his possession to obtain access to the protected communication; and

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

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

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

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

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

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

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

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

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

(5) Where—

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

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

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

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

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

(*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 shall be liable upon conviction before a Resident Magistrate to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding six months, or to both such fine and imprisonment.

(8) An authorized 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, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the communication or put it into an intelligible form; and

(*c*) the number of—

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

(ii) copies made of the key,

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

(9) An authorized officer who knowingly contravenes subsection (8) commits an offence and upon summary conviction before a Resident Magistrate shall be liable to a fine not exceeding one million dollars or to imprisonment for a term not exceeding twelve months, or to both such fine and imprisonment.

Admissibility of evidence.

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

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

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

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

(3) In any criminal proceedings—

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

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

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

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

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

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

the Court may exclude such disclosure.

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

Offences.

15.—(1) A person who, in an application or affidavit under this Act, makes a statement which he knows to be false in any material particular commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to a fine not exceeding three million dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(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 authorized to disclose the communication; or

(*b*) obtained in contravention of this Act,

commits an offence, whether the disclosure takes place in Jamaica or elsewhere, and is liable upon summary conviction in a Resident Magistrate's Court to a fine not exceeding five million dollars or to imprisonment for a term not exceeding five years, or to both such fine and imprisonment.

21/2011 S. 3(a).

(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) In the case of an offence under subsection (2), where the disclosure takes place outside of Jamaica, the Resident's Magistrate Court for the Corporate Area shall have jurisdiction to hear the matter.

21/2011 S. 3(b).

Disclosure of communications data.

16.—(1) In this section—

"communications data" means any—

(*a*) traffic data comprised in or attached to a communication, whether by the sender or otherwise, for the purposes of any telecommunications network by means of which the communication is being or may be transmitted;

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

(i) of any telecommunications network; or

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

"designated person" means the Minister or any person prescribed for the purposes of this section by the Minister by order subject to affirmative resolution;

"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 purposes 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.

(1A) For the avoidance of doubt, the information referred to in paragraph (*b*) of the definition of "traffic data" includes information as to the means and source of payment for the telecommunications service (including any relevant credit card numbers or bank account numbers). 39/2013 S. 39(4)(*a*)(i).

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

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

(*b*) if the provider is not already in possession of the data, to obtain the data and so disclose it.

(3) A designated person shall not issue a notice under subsection (2) or (3A) in relation to any communications data unless he is satisfied that it is necessary to obtain that data— 39/2013 S. 39(4)(*a*)(ii).

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

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

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

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

39/2013
S. 39(4)(*a*)(iii).

(3A) Where it appears to a person listed in column A of the Second Schedule that—

(*a*) the provider of a telecommunications service is or may be in possession of, or capable of obtaining, any communications data; and

(*b*) it is necessary to obtain that data for any purpose specified in relation thereto in column B of the Second Schedule,

the person may issue to the provider a notice in writing requiring the provider to disclose to a specified person named in the notice all of the data in the provider's possession or subsequently obtained by the provider or, if the provider is not already in possession of the data, to obtain the data and so disclose it.

39/2013
S. 39(4)(*a*)(ii).

(4) A notice under subsection (2) or (3A) shall state—

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

39/2013
S. 39(4)(*a*)(iv).

(*b*) the authorized officer (or specified person, in the case of a notice issued under subsection (3A) to whom the disclosure is to be made;

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

(*d*) the matters falling within subsection (3) by reference to which the notice is issued; and

(*e*) the date on which it is issued.

(5) A notice under this section shall not require—

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

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

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

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

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

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

(*b*) an attorney-at-law for the purpose of obtaining legal advice or representation in relation to the notice,

and a person referred to in paragraph (*a*) or (*b*) shall not disclose the existence or operation of the notice , except to the authorized officer specified in the notice or for the purpose of—

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

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

(9) A person who obtains communications data pursuant to a notice under this Act shall not disclose any such data, except— 39/2013 S. 39(4)(*a*)(v)(A).

(*a*) as permitted by the notice;

(*b*) in connection with the performance of his duties; 39/2013 S. 39(4)(*a*)(v)(B).

39/2013 S. 39(4)(*a*)(v)(B).

(*c*) in the case of communications data obtained pursuant to a notice under subsection (3A), in accordance with the provisions of the Securities Act which permit such disclosure to an agency of a foreign Government for the purpose of cooperation in the enforcement of laws pertaining to the regulation of the securities sector;

39/2013 S. 39(4)(*a*)(v)(B).

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

(10) A person who contravenes subsections (7), (8) or (9) commits an offence and is liable on summary conviction in a Resident Magistrate's Court to a fine not exceeding five million dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

Admissibility of communications data.

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

(2) In admitting into evidence any communications data 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 16 shall be sufficient disclosure as to the source or origin of the data; and

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

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

(*a*) the disclosure would jeopardize the course of any investigations being carried out by authorized officers; and

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

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

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

Amendment of Schedule. 39/2013 S. 39(4)(*b*).

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

19. 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.

Regulations.

39/2013
S. 39(4)(*c*).

FIRST SCHEDULE (Sections 4 and 18)

Applicable Offences

1. Capital or non-capital murder or treason.

2. Kidnapping or abduction.

26/2013
2nd Sch.

3. An Offence contrary to section 92 (Concealment, *etc.*, criminal property) or section 93 (Acquisition, use and possession of criminal property) of the Proceeds of Crime Act.

4. Producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the Dangerous Drugs Act.

5. Transporting or storing a dangerous drug where possession of such drug contravenes the Dangerous Drugs Act.

6. Importing or exporting a dangerous drug in contravention of the Dangerous Drugs Act.

7. Importation, exportation or transshipment of any firearm or ammunition in contravention of the Firearms Act.

8. Manufacture of, or dealing in, firearms or ammunition in contravention of the Firearms Act.

9. Illegal possession of a prohibited weapon or any other firearm or ammunition contrary to section 20 of the Firearms Act.

10. An offence contrary to section 14 of the Corruption Prevention Act.

11. Arson.

17/2006
S. 5.

12. A terrorism offence, as defined by section 2 of the Terrorism Prevention Act.

17/2006
S. 5.

13. An offence under section 10 of the Child Care and Protection Act (sale or trafficking of children).

12/2009
3rd Sch.

14. An offence contrary to section 69 (child stealing) of the Offences Against the Person Act.

3/2010
S. 22.

15. Any offence under Part II of the Cybercrimes Act.

3/2010
S. 22.

16. Aiding, abetting or conspiring to commit any of the offences mentioned in paragraphs 1 to 15.

SECOND SCHEDULE (Section 16) 39/2013 S. 39(4)(*c*).

Column A	Column B
Person who may require data	*Purpose of requiring data*
The Executive Director of the Financial Services Commission.	The prevention or detection of any offense referred to in section 68E of the Securities Act, if the Executive Director is satisfied that there are reasonable grounds for believing that— (*a*) such an offence has been, is being or is about to be committed; and (*b*) the sender or recipient of any communication, or the subcriber to the telecommunications service, to which the data relates, is the subject of an investigation in connection with the offence.