INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATION MESSAGES BILL, 2016

ARRANGEMENT OF SECTIONS

Section

1. Application
2. Purposes for interception
3. Prohibition of unlawful interception
4. Procedure for interception
5. Application for authorisation for a warrant
6. Receipt of application
7. Conditions for interception warrant for criminal investigation
8. Conditions for interception warrant for security reasons
9. Contents of an interception warrant
10. Unauthorised disclosure
11. Duration, cancellation and extension of interception warrant
12. Modification of an interception warrant
13. Enforcement of an interception warrant
14. Interception capability
15. Compliance with requirement for interception capability
16. Matters relating to design of network
17. Cost of interception capability
18. Ministerial responsibility
19. Reporting to Parliament
20. Regulations
21. Interpretation
22. Consequential amendments, repeal and savings

A

BILL

ENTITLED

INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATION MESSAGES ACT, 2016

AN ACT to provide for the interception of postal packets, telephone or other electronic or cyberspace communication for the purpose of protecting national security, fighting crime generally and in particular suppressing organised crime including money laundering, terrorism, narcotic trafficking and other serious offences and for related matters.

PASSED by Parliament and assented to by the President:

Application

1. This Act applies only to public postal services and public telephone or other electronic or cyberspace communication services.

Purposes for interception

2. Subject to clause 2 of article 18 of the Constitution, a person may for the purpose of

(a) protecting national security,
(b) fighting crime generally,
(c) suppressing organised crime, including money laundering, terrorism or narcotic trafficking, or
(d) other serious offence

intercept a postal packet, telephone message or other electronic or cyberspace communication message that that person has lawful authority to intercept.

Prohibition of unlawful interception

3. (1) A person shall not without lawful authority intentionally intercept a postal packet, telephone message or other electronic or cyberspace communication message in the course of the transmission or storage of the postal packet or message.

(2) A person who contravenes subsection (1) in relation to

(a) a postal packet commits an offence and is liable on summary conviction to a fine of not more than two hundred and fifty penalty units or to a term of imprisonment of not more than two years or to both.

(b) a telephone or other electronic or cyberspace communication message commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

(3) For the purpose of subsection (1), interception is with lawful authority if it is done in accordance with

(a) sections 30 and 31 of the Postal and Courier Services Regulatory Commission Act, 2003 (Act 649); or

(b) this Act.

(4) Subsection (2) does not limit the right of a person affected by an interception of a postal packet or telecommunication message without lawful authority to seek redress by a civil suit in court.

Procedure for interception

4. (1) Where there is the need to intercept a postal package, telephone, other electronic or cyberspace communication message the National Security Co-ordinator shall on the authority of the Minister, subject to the conditions specified under sections 7 and 8, obtain a warrant for that purpose from a Justice of the High Court sitting in camera.

(2) A person to whom an interception warrant is addressed shall in the manner described in the warrant

(a) secure the interception of a postal packet or a telecommunication message in the course of the transmission or storage of the packet or message;

(b) cause a request to be made in accordance with an international mutual assistance agreement for provision of assistance in connection with, or in the form of an interception of a postal packet or telecommunication message; or

(c) secure the disclosure of material obtained by interception under the warrant.

(3) Despite subsection (2), the National Security Co-ordinator may where there is the need for urgency, authorise in writing the interception without a warrant of a postal packet or telecommunication message but the written authorisation shall be confirmed by obtaining a warrant from the High Court within forty-eight hours after the written authorisation has been issued.

(4) Where a written authorisation is not confirmed within the forty-eight hour period, the authorisation shall cease to have effect and any

(a) interception carried out after the refusal of confirmation of the written authorisation is unlawful; and

(b) information obtained shall not be used against the person in a court of law.

Application for authorisation for a warrant

5. (1) For the purpose of coordinating applications for an interception warrant the National Security Co-ordinator shall grant an authorisation to obtain the warrant.

(2) A public officer who desires to obtain an interception warrant from a Justice of the High Court on behalf of the following persons shall apply to the National Security Co-ordinator

(a) the National Security Council Secretariat;

(b) the Director of the Bureau of National Investigation;

(c) the Inspector-General of Police;

(d) the Commissioner-General of the Ghana Revenue Authority;

(e) the Director-General, Defence Intelligence;

(f) the Executive Director, Economic and Organised Crime Office;

(g) the Executive Secretary, Narcotics Control Board;

(h) the Comptroller-General of the Ghana Immigration Service;

(i) the Chief Executive Officer of the Financial Intelligence Centre;

(j) the Chief Director of the Ministry of Foreign Affairs; or

(k) any other person who for the purposes of an international mutual legal assistance agreement is the competent authority of a foreign country.

(3) The application for authorisation shall be in writing and submitted by the public officer

(a) authorised for that purpose where it is made on behalf of any of the persons specified in subsection (2); or

(b) nominated for the purposes of the authorisation by the National Security Co-ordinator.

(4) The application shall include sufficient information to enable the National Security Co-ordinator determine whether the conditions required for the grant of authorisation to obtain an interception warrant have been satisfied.

Receipt of application

6. (1) A public officer nominated by the National Security Co-ordinator shall receive applications for authorisation for obtaining an interception warrant.

(2) The officer shall

(a) consider the application and make any inquiries that are necessary; and

(b) submit to the National Security Co-ordinator a report signed by that officer, stating in the opinion of the officer, whether or not the conditions required for an interception warrant have been satisfied.

(3) For the purpose of subsection (2), information that is available to the officer at the time of receipt of the application or that becomes available after the receipt of the application but before the grant of the authorisation may be considered to be included in the application.

(4) Where the officer is for any reason absent from Office, the National Security Co-ordinator may designate another officer to perform the functions specified under this section.

Conditions for interception warrant for criminal investigation

7. The conditions for the issue of an interception warrant for the purpose of criminal investigation including investigation of money laundering, drug trafficking, terrorism, financing of terrorism, proliferation of weapons of mass destruction and other serious offences are as follows:

(a) the investigations are being conducted by a public institution charged with the investigation of the offences referred to in this section;

(b) the investigations have failed or are likely to fail to yield information to show that the offence has been committed or there is insufficient evidence or information for the purpose of instituting proceedings in relation to the offence;

(c) there is reasonable ground to believe that the interception of a postal packet sent to a particular address or of a telecommunication message sent to or from a particular address would be of material assistance in providing information or evidence for the purpose of proceedings in relation to an offence or in preventing or detecting an offence;

(d) in the case of a serious offence that is likely to be committed, it is necessary for investigations to be carried out by a public institution charged with the prevention or investigation of the offence involved for the purpose of detecting or preventing the commission of the offence;

(e) investigations carried out without interception have failed, or are likely to fail to yield information on the perpetrators, the time, the place and other circumstances of the offence in order to prevent the Commission of the offence or identify the perpetrators; or

(f) the circumstances of the case are sufficient to justify the interception having regard to the importance of obtaining the information or evidence in comparison with the need to preserve the privacy of a postal packet or telecommunication message.

Conditions for interception warrant for security reasons

8. The conditions required to be satisfied for the issue of a warrant of interception on grounds that the interception is in the interest of the security of the State are that

(a) there are reasonable grounds to believe that a particular activity which is endangering or likely to endanger the security of the State is being carried on or has been planned to be carried on;

(b) investigations are being conducted by or on behalf of the person applying for the warrant for the purpose of ascertaining whether an activity that is endangering or likely to endanger the security of the State

(i) is in fact being carried on; or

(ii) is planned to be carried on and by whom and the nature and extent of the activity;

(c) investigations that do not involve interception have failed or are likely to fail to provide information to show that the activity is being carried on or planned to be carried on;

(d) there are reasonable grounds to believe that the interception of a postal packet sent to a particular address or of a telecommunication message sent to or from a particular address will provide material assistance in providing the required information.

Contents of an interception warrant

9. (1) An interception warrant shall

(a) bear the date on which the authorisation to which the interception warrant relates was given;

(b) state whether the proposed interception is in relation to a postal packet or telecommunication message or both;

(c) state that the requirements of this Act in relation to the authorisation to which the warrant relates have been complied with;

(d) specify the postal address and where necessary the person to whom the proposed interception relates, the telecommunication address or cyber address to which the proposed interception relates; and

(e) set out the numbers, apparatus or other factors that are to be used to identify the postal packet or telecommunication message that is to be intercepted.

(2) The interception warrant may require the person to whom the warrant is addressed to disclose the intercepted material to a person specified in the warrant.

Unauthorised disclosure

10. (1) The following persons shall keep confidential matters referred to in subsection (2) in relation to an interception warrant that has been issued or extended:

(a) the persons specified in section 5 (2);
(b) a public officer;
(c) an employee of the National Security Council Secretariat;
(d) an employee of the Criminal Investigations Department of the Ghana Police Service;
(e) an employee of the Bureau of National Investigations;
(f) an employee of the Economic and Organised Crime Office;
(g) an employee of the Financial Intelligence Centre;
(h) a provider of postal services or a person employed for the purpose of the business of providing a postal service;
(i) a provider of cyberspace communication services or a person employed for the purpose of the business of providing a cyberspace communication service;
(j) an employee of the Ghana Immigration Service;
(k) an employee of the Narcotics Control Board;
(l) an employee of the Ghana Revenue Authority
(m a provider of telecommunication services or a person employed for the purpose of the business of providing a telecommunication service; and
(n) a person who has control of the whole or a part of a telecommunication system located wholly or partly in this country.

(2) The matters required to be kept confidential are

(a) the existence and contents of an interception warrant;
(b) the details of the issue of the warrant and of any extension or modification of the warrant;

(c) the existence and content of a requirement to provide assistance to give effect to the warrant;
(d) the steps taken in pursuance of the warrant or of a requirement to provide assistance to give effect to the warrant; and
(e) any other thing in the intercepted material.

(3) A person who discloses a matter which that person is required to keep confidential commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

(4) In any proceedings against a person for an offence under subsection (3), it is a defence for that person to show that

(a) the disclosure was made by or to a professional legal adviser for the purpose of giving advice to a client about the effect of the provisions of this Act;
(b) the person to whom or, as the case may be, by whom the disclosure was made was the client or a representative of the client mentioned in paragraph *(a)*;
(c) the disclosure was made to a legal adviser in contemplation of, or in connection with, any legal proceedings;
(d) that person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure;
(e) the disclosure was confined to a disclosure made to the High Court Judge appointed to supervise matters in respect of interception warrants or was authorised
  (i) by the High Court Judge;
  (ii) by the warrant or the person to whom the warrant is or was addressed; or
  (iii) by the terms of the requirement to provide assistance.

Duration, cancellation and extension of an interception warrant

11. (1) An interception warrant is valid for three months after the date of issue and may be extended.

(2) The National Security Co-ordinator may where necessary apply to the High Court by motion ex-parte to obtain an extension of an interception warrant but the extension shall not exceed three months at a time.

(3) The hearing of an application relating to an interception warrant in subsection (2) shall be held in camera.

(4) An application for an extension of an interception warrant is subject to the same conditions for the issue of the interception warrant.

(5) Each interception warrant shall have a unique number and where the interception warrant is extended it shall bear the same unique number.

(6) The National Security Co-ordinator shall apply to the High Court by motion ex-parte to cancel an interception warrant where the reasons for the issue of the interception warrant no longer exists.

(7) Where an interception warrant is cancelled under subsection (6), the National Security Co-ordinator shall notify the person to whom the warrant was addressed of the cancellation.

Modification of an interception warrant

12. (1) The National Security Co-ordinator may apply to the High Court by motion ex-parte to modify an interception warrant where

(a) a matter that ought to have been included in the interception warrant has not been included; or

(b) a matter that has been included in the interception warrant

(i) has ceased to be relevant or necessary; or

(ii) ought not to have been included.

(2) Where an interception warrant is modified it shall bear the same unique number as that of the original interception warrant.

Enforcement of an interception warrant

13. (1) An interception warrant may be enforced by

(a) the person to whom the interception warrant is addressed; or

(b) the person to whom the warrant is addressed, acting through or together with another person required to assist in enforcing the warrant.

(2) A person to whom an interception warrant is addressed may for the purpose of requiring another person to provide assistance in relation to the interception warrant,

(a) serve a copy of the warrant on that other person who is required to give the assistance; or

(b) arrange for a copy of the warrant to be served on that other person.

(3) Where a copy of an interception warrant is served on a person who

(a) provides a postal service;

(b) provides a telecommunication service or cyberspace telecommunication service; or

(c) does not provide a telecommunication service but who has control of the whole or part of a telecommunication system located in this country,

that person shall take the necessary action to enforce the warrant in the manner specified in the warrant.

(4) A person who contravenes subsection (3) commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

Interception capability

14. (1) The National Security Co-ordinator may, in furtherance of an interception warrant, request a person who provides or is seeking to provide

(a) a public postal service;

(b) cyber communication service; or

(c) a public telecommunication service

to take steps that are necessary for the enforcement of an interception warrant.

(2) The request shall be in writing and specify the steps to be taken by that person to obtain the necessary practical interception capability to enforce an interception warrant.

(3) The determination of the practical capability of that person to provide assistance in relation to an interception shall include measures that the National Security Co-ordinator considers necessary

(a) with respect to the disclosure of intercepted material; and

(b) for the purpose of ensuring the maintenance of security and confidentiality in relation to

(i) the provision of the assistance; and

(ii) matters connected to the provision of the assistance.

(4) The steps required to be taken in respect of practical interception capability under subsection (2) include the development, installation and maintenance of equipment that is necessary for carrying out an interception by the person to whom the request is addressed.

(5) In the development, installation and maintenance of equipment for the purpose of practical interception capability the person to whom the request is addressed shall apply the best international standards.

(6) For the purpose of subsection (5), "best international standards" means the standards of the European Telecommunication Standards Institute.

(7) A person who is required to install and who installs equipment for the purpose of interception capability shall keep the existence of the equipment and packets or messages intercepted by means of the equipment secret and confidential.

(8) Equipment installed for the purpose of interception capability in this country shall not be

(a) installed, managed or monitored in a foreign country; or

(b) capable of being remotely accessed from a foreign country for the purpose of maintenance.

(9) A person appointed to maintain an equipment for ensuring interception capability shall be subject to security clearance determined by the National Security Co-ordinator.

(10) A person is not liable to a civil suit under this Act if that person

(a) on request, installs an equipment for the purpose of ensuring interception capability;

(b) is appointed to maintain an equipment for ensuring an interception capability; or

(c) makes a postal packet or telecommunication message available to a competent authority.

Compliance with requirement for interception capability

15. (1) For the purposes of this Act, a person required to provide and maintain interception capability has that capacity if another person acting on the authority of an interception warrant is able to

(a) identify and intercept the postal packet or telecommunication message which is the subject of the interception warrant;

(b) obtain call associated data

(i) relating to a telecommunication message which is permitted to be intercepted under this Act; and

(ii) together with the content of the telecommunication message which is permitted to be intercepted under this Act;

(c) carry out the interception of a postal packet or telecommunication message in a manner that

(i) does not unduly interfere with any other postal packet or telecommunication message; and

(ii) protects the privacy of any other postal packet or telecommunication message which is not the subject of an interception warrant.

(2) Where a person required to provide and maintain interception capability undertakes the interception of a postal packet or a telecommunication message on behalf of a body or a person authorised under an interception warrant, the interception is complete when

(a) the postal packet, or

(b) the call associated data or the content of the telecommunication message or both

are submitted to the body or person authorised under the interception warrant.

(3) Subject to subsection (4), a person required to provide and maintain an interception capability shall, in furtherance of subsection (l)(b)(ii) decrypt a telecommunication message being transmitted by the network or service of that person

(a) if the content of that telecommunication message is encrypted; and

(b) that person provided the keys.

(4) Subsection (3) does not impose an obligation on a person required to provide and maintain an interception capability to

(a) decrypt a telecommunication message transmitted by the network or service of that person if the encryption is provided by means of a product that is supplied by that person as an agent for that product; or

(b) ensure that a body or person issued with an interception warrant has the ability to decrypt a telecommunication message.

Matters relating to design of network

16. A person acting on the authority of an interception warrant issued under this Act or any other enactment shall not

(a) prohibit another person from adopting a specific design or feature for a telecommunication network; or

(b) require another person to adopt a specific design or feature for a telecommunication network.

Cost of interception capability

17. A person who, upon a request to provide interception capability installs an equipment to enable that person to provide the interception capability shall bear the cost of the installation or modification.

Ministerial responsibility

18. The National Security Co-ordinator shall in the performance of functions under this Act, be answerable to the Minister.

Reporting to Parliament

19. (1) The Minister shall submit annual reports to Parliament on the implementation of this Act.

(2) The report submitted under subsection (1) shall not contain any information

(a) prejudicial to the prevention or detection of crime; or

(b) detrimental to the security of the State; and

(c) shall in particular exclude the names of the service providers who are providing assistance for the enforcement of the interception warrant.

Regulations

20. The Minister on the advice of the National Security Co-ordinator may, by legislative instrument, make Regulations that are necessary for the implementation of this Act.

Interpretation

21. In this Act unless the context otherwise requires

"call associated data" includes

(a) information

(i) that is generated as a result of the making of or sending a telecommunication message whether or not the telecommunication message is sent or received successfully; and

(ii) that identifies the origin,

(b) the identifying address or addresses from which the telecommunication message originates;

(c) the identifying address or addresses to which the telecommunication message is sent;

(d) the numbers, where the telecommunication message is diverted from one number to another number;

(e) the time at which the telecommunication message is sent or received; and

(f) the duration of the telecommunication message, the point at which the telecommunication message first enters a network, but does not include the content of the telecommunication message;

"intercept" includes to hear, listen to, record, monitor, acquire, receive, intercept, divert or tamper with a telecommunication message

(a) while the telecommunication message is taking place on a telecommunication network; or

(b) while the telecommunication message is in transit on a telecommunication network and the dispatch, transmission and receipt of a postal packet;

"interception capability" means the capability to intercept a postal packet or telecommunication message as described in this Act;

"interception warrant" means a warrant that is issued by a judge under this Act, for the purpose of interception of a postal packet or telecommunication message;

"Minister" means the Minister responsible for the Interior;

"network" means the collection of terminal nodes, links and any intermediate nodes which are connected to make the transmission of a telecommunication message possible and also includes devices that manage the flow of and retention of information;

"public officer" means an officer, agent, employee or other representative of a public entity acting in the course of duty as an officer, agent, employee or representative of the public entity;

"public telecommunication service" means any telecommunication service which is offered or provided to the public;

"serious offence" includes

(a) participation in an organised criminal group, terrorism and terrorist financing, money laundering, human trafficking, people smuggling, rape, defilement, illicit trafficking in stolen and other goods, corruption and bribery, serious fraud, counterfeiting and piracy of products, smuggling, extortion, forgery, insider trading and market manipulation;

(b) murder, grievous bodily harm, armed robbery or theft where these are predicate offences for a serious offence; and

(c) any other similar or related, prohibited activity punishable with imprisonment for a period of not less than twelve months;

" telecommunication service" means any service that consists in the provision of access to, and of facilities for making use of any telecommunication system whether or not one provided by the person providing the service;

"telecommunication system" means any system which exists either wholly or partly in the country or elsewhere for the purpose of facilitating the transmission of communication by any means involving the use of electrical, optical or electro-magnetic energy;

"telecommunication message" includes telephone message or other electronic or cyberspace communication message and the content and associated data of that message or communication; and

"warrant" means interception warrant.

Consequential amendments, repeal and savings

22. (1) Where in an enactment, provision is made for the interception of a postal packet or telecommunication message, that power shall be exercised in accordance with this Act and with the necessary modifications.

(2) Section 100 of the Electronic Communications Act, 2008 (Act 775) is repealed.

(3) Despite the repeal in subsection (2), any instrument issued or order made under the repealed provision shall continue to be in force until it is revoked.

Date of *Gazette* notification: 16th June, 2016

GPCL, ASSEMBLY PRESS, ACCRA. GPCL/A444/450/06/2016
Website: www.ghpublishingcompany.com E-mail: info@ghpublishingcompany.com

INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATION MESSAGES BILL, 2016

MEMORANDUM

The object of the Bill is to enact legislation for the lawful interception of postal packets and telecommunication messages for the purpose of fighting crime, suppressing organised crime including money laundering, terrorism, narcotic trafficking, identity theft and generally for the protection of national security.

Article 12 of the 1992 Constitution of the Republic of Ghana provides as follows:

"Protection of Fundamental Human Rights and Freedoms

12. (1) The fundamental human rights and freedoms enshrined in this Chapter shall be respected and upheld by the Executive, Legislature and Judiciary and all organs of Government and its agencies and, where applicable to them, by all natural and legal persons in Ghana, and shall be enforceable by the Courts as provided for in this Constitution.

(2) Every person in Ghana, whatever his race, place of origin, political opinion, colour, religion, creed or gender shall be entitled to the fundamental human rights and freedoms of the individual contained in this Chapter, but subject to respect for the rights and freedoms of others and for the public interest."

Article 18 (2) also provides that

"(2) No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well being of the country, for the protection of health or morals, for prevention of disorder or crime or for the protection of the rights or freedoms of others."

These constitutional provisions demonstrate the importance of fundamental human rights and freedoms generally and of the right of the individual to privacy, in particular.

Ordinarily the right to privacy as a fundamental human right should not be tampered with unless there are special reasons relating to the protection of the rights and freedoms of others, the public interest or the prevention of disorder or crime that necessitates their being tampered with and even then this must be done under an Act of Parliament.

Thus to interfere with the right of privacy as the draft Bill seeks to do now, circumstances that require that interference must exist.

A few years back, the scourge of terrorism, proliferation of weapons of mass destruction and drug trafficking on a massive scale were unknown in the West African subregion. Currently, however, the existence of Boko Haram in Nigeria and the current actions of ISIS in neighbouring Cote D'Ivoire have brought the issue of terrorism close to our doorsteps. In addition, the West African subregion has within a short time been turned into a hub for the narcotic drug trafficking trade. The activities of the terrorist organisations as the example of Boko Haram in Nigeria shows, affect the well being of ordinary people who are maimed and killed through the violence unleashed by the terrorists at large. Apart from such activities creating disorder, fear and insecurity, they also undermine the confidence of investors in the economy in which they take place.

The issue of armed robbery, terrorism, money laundering and narcotic drug trafficking has become a real threat to public order and to the safety and well-being of individual citizens in Ghana as well as in West Africa as a whole.

The illicit or narcotic drug trade also hurts the human resource in the country in which it occurs because it is the youth of the country who become victims. To counter the effects of these activities there have been many United Nations Resolutions such as Security Council Resolution 1373 (2001).

Ghana is a State party to most of these Conventions and is obliged under these Conventions to take steps to fight such nefarious activities. In this regard, a number of laws have been enacted to tackle these activi ties. Among these laws are the Anti-Money Laundering Act, 2008 (Act 749), the Anti Terrorism Act, 2008 (Act 762) and the Economic and Organised Crime Office Act, 2010 (Act 804). In spite of these enactments those involved in the activities prescribed under them continue to operate with some amount of freedom. This freedom of operation has become possible because of developments in information technology which have made communication relatively easy and to a certain extent anonymous.

INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATION MESSAGES BILL, 2016

The emergence of new forms of communications such as electronic mail and social media have presented the security and intelligence agencies with new challenges. These challenges make monitoring of communications of identified criminals by the security and intelligence agencies almost impossible in real time. Again most telecommunication service providers do not keep track of the sites that their customers visit or have any easy way of correlating particular communication traffic with an individual. Furthermore, the lack of oversight and absence of a sanctions regime for unlawful interception may result in the infringement of the privacy right of citizens.

Although existing legislation provide measures for interception, there are inconsistencies that border on the multiplicity of fora, procedure and authorisation relating to an application for an order to intercept. The existing laws do not also have provisions requiring the telecommunication service providers to have interception capability thereby making it impossible to execute orders granted by the courts for interception of communication.

Since the fundamental right of freedom of privacy is involved there is the need for law not only to permit the interference with the right but also to establish a transparent mechanism which is subject to due process to ensure that the right in question is not unduly abused.

This Bill therefore seeks to provide for a centralised judicial process for purposes of intercepting communication of persons suspected of criminal activity and also to consolidate all the powers of interception, currently scattered in multiple legislation. It will also ensure that the telecommunication service providers provide an interception capability which would make it possible to intercept communication in real time and provide the security and intelligence agencies the ability to trace the communications of criminals over cell phones, computer networks and new technologies that may be developed.

Clause 1 of the Bill deals with the application of the law and provides that interception of postal packets or a telephone message applies only to public postal services and public telecommunication services.

Clause 2 specifies the purposes for which interception of postal packets, telephone or other electronic or cyberspace communication is legally permissible. Some of these purposes are criminal investigation, suppression of organised crime such as money laundering and the protection of the security of the State.

Clause 3 prohibits the interception of a postal packet, telephone or other electronic or cyberspace communication unless the interception is lawful and done in accordance with the Postal and Courier Services Regulatory Commission Act, 2003 (Act 649) or the Act. Any person who intercepts a postal packet, telephone or other electronic or cyberspace communication without lawful authority commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both the fine and imprisonment.

Clause 4 specifies the procedure for interception. Interception cannot be carried out legally unless a warrant is obtained for that purpose from a Justice of the High Court.

C*lause* 5 provides that for purposes of co-ordinating applications for interception warrants, a public officer of a specified agency may apply to the National Security Co-ordinator to obtain a legal interception warrant from the High Court.

Provision is made under c*lause* 6 for receipt of application for authorisation whilst *clauses* 7 and 8 deal with conditions for which an interception warrant is to be granted in respect of criminal investigation and in circumstances where interception is in the interest of the security of the State.

Clause 9 caters for the contents of an interception warrant. An interception warrant is legal if it satisfies the conditions for the issue of the warrant, bears a date, states whether the proposed interception is in relation to a postal packet, telephone or other electronic or cyberspace communication or a combination and specifies the address or the person to whom the proposed interception relates.

Clause 10 deals with unauthorised disclosure of the existence and contents of an interception warrant among other matters. A person who discloses a matter that is to be kept secret or confidential as regards an interception warrant commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both the fine and the imprisonment.

The duration, cancellation and extension of an interception warrant are provided for in *clause* 11. An interception warrant is valid for three months but may be extended where necessary. It may also be cancelled by an application to the designated High Court Judge where the reasons for the issue of the warrant cease to exist.

Under *clause* 12 an interception warrant may be modified to include a matter that ought to have been included in the warrant or delete other matters that should not have been included in the warrant. An interception warrant shall be enforced by the security agency responsible for carrying out interception with the assistance of the service provider on whose platform or through whose system the target communication is made together with any other person required to assist in enforcing the warrant, *clause* 13.

Clauses 14, 15 and 16 deal with interception capability, compliance with requirement for interception capability and matters relating to design of network. In *clause* 17, provision is made for the cost of interception capability. The cost of an interception capability is to be borne by the person who installs the equipment to provide the interception capability.

Under *clause* 18, the National Security Co-ordinator is mandated to report to the Minister responsible for the Interior in the performance of functions under the Act whilst *clause* 19 requires the Minister to submit annual reports to Parliament.

The enabling power of the Minister to make Regulations is provided for under *clause* 20. *Clause* 21 is on interpretation whilst *clause* 22 deals with repeals, savings and consequential amendments.

Interception of Postal Packets and Telecommunication Messages Bill, 2016

The Bill when passed into law, will be an additional tool to respond to current threats which are urgent and require prompt action and generally enhance the security of the country.

HON. PROSPER DOUGLAS BANI
Minister responsible for the Interior

Date: 15th June, 2016.