

DRAFT

Interception of Communications Bill, 2006

MEMORANDUM

The purpose of this Bill is to establish an interception of communication monitoring centre and for the appointment of persons to that centre whose function shall be to monitor and intercept certain communications in the course of their transmission through a telecommunication, postal or any other related services system. In more detail the Bill provides as follows:

PART I

The Bill's short title is set out in clause 1. Clause 2 defines the terms that are used throughout the Bill.

PART II

This Part will establish a monitoring centre which shall be the sole facility through which authorised interceptions shall be effected. The centre shall be controlled and operated by designated technical experts.

PART III

The persons who are authorised to make applications for interception of communications include the Chief of the Defence Intelligence, the Director-General of the President's department of national security, the Commissioner of the Zimbabwe Republic Police and the Commissioner-General of the Zimbabwe Revenue Authority. Under this Part the Minister is authorised to issue an interception warrant to authorised persons where there are reasonable grounds for the Minister to believe (among other things) that a serious offence has been or is being or will probably be committed or that there is threat to safety or national security of the country. The warrant issued by the Minister shall be valid for a period not exceeding three months and must specify the name and address to which the interception shall take place. Any communication which has been intercepted in terms of any warrant shall not be disclosed to any other person with the exception where the information may be required in any proceedings in any court. No court shall accept as evidence where such evidence has been obtained by means of any interception committed in contravention of this Act. Furthermore a telecommunication service provider is required to install hardware and software facilities and devices to enable interception of communications and also that the telecommunication service can store communication-related information and how the service could be connected with the communication monitoring centre or the manner in which information can be re-routed to the monitoring centre. The telecommunication service provider shall be assisted or compensated for the assistance he or she may provide to the Authority or the monitoring centre.

PART IV

This Part will provide for the general prohibitions and exemptions from disclosure of any information which an individual may have obtained in the exercise of his or her duties in terms of this Act. Only authorised persons who execute an interception or assist with the execution of any intercepted communication may disclose such contents to the extent that such disclosure is necessary for the proper performance of the official duties of the authorised person. The authorised person is also required to destroy as soon as possible after use any intercepted material. Authorised persons may also make applications to the for a detention order to detain any postal article where the authorised person has reasonable suspicion that that article in the custody of a licensee contains anything in respect of which an offence or attempted offence is being committed.

Any person who may be aggrieved by a decision made by the Authority, authorised person may appeal to the Minister and the Minister may confirm, vary or set aside the decision

appealed against. If an aggrieved person is not satisfied with the decision of the Minister, he or she may appeal against it to the Administrative Court.

The Minister under this Part is empowered to make regulations providing for all matters which by this Act are required to be prescribed or which in his opinion, are necessary or convenient to be prescribed.

DRAFT

Interception of Communications Bill, 2006

Arrangement of Sections

PART I

PRELIMINARY

Section

1. Short title.
2. Interpretation.

PART II

CONTROL OF INTERCEPTION AND ESTABLISHMENT OF A MONITORING CENTRE

3. Control of interception.
4. Monitoring centre.

PART III

APPLICATION FOR LAWFUL INTERCEPTION OF COMMUNICATIONS

5. Authorised persons to make an application for interception.
6. Issue of warrant.
7. Scope of warrant.
8. Nondisclosure
9. Evidence obtained by unlawful interception not admissible in criminal proceedings.
10. Assistance by postal and telecommunications service providers
11. Duties of telecommunication service provider and customer.
12. Notice of disclosure of information protected by security key.
13. Interception capability of telecommunication service.
14. Compensation payable to postal service provider or telecommunication service provider or protected information key holder.

PART IV

GENERAL PROHIBITIONS AND EXEMPTIONS

15. General prohibitions and exemptions.
16. Disclosure of information by authorised persons.
17. Disposal of intercept product.
18. Application for a detention and examination order.
19. Examination and accountability for detained postal articles.
20. Appeals.
21. Regulations

PRESENTED BY THE MINISTER OF TRANSPORT AND COMMUNICATIONS

DRAFT

BILL

To provide for the lawful interception and monitoring of certain communications in the course of its transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of the monitoring centre; and to provide for any other matters connected with or incidental to the foregoing.

ENACTED by the President and the Parliament of Zimbabwe.

PART I

PRELIMINARY

1. Short title

This Act may be cited as the Interception of Communications Act [Chapter]

2. Interpretation

“access” means the technical ability to interface with a communications facility such as a telecommunications line or switch to enable the interception of any communication carried on that facility;

“Agency” means the government telecommunications agency comprising telecommunications experts which has been designated to operate the monitoring facility and which give technical directions to service providers so as to ensure compliance of the provisions of this Act;

“Authority” means the Postal and Telecommunications Authority established by section 3 of the Postal and Telecommunications Act [Chapter 12:05] (Act No. 4 of 2000).

“authorised persons” means persons referred to in section 5

“call” means any connection fixed or temporary capable of transferring information between two or more users of a telecommunications system;

“call-related information” includes switching, dialling or signalling information that identifies the origin, destination, termination duration and equipment identification of each communication generated or received by customer or user of any equipment, facility or service provided by a service provider and where applicable, the location of the user within the telecommunications system;

“customer” means—

- (a) any person, body or organisation which has entered into a contract with the service provider for the provision of a telecommunication service to that person, body or organisation; or
- (b) any person to whom or any body or organisation to which a service provider provides a pre-paid telecommunication service;

“intercept”, in relation to communication which is sent by—

- (a) means of a telecommunication system or radio communication system means to listen to, record, or copy whether in whole or in part;

(b) post, means to read or copy the contents, whether in whole or part;

“interception interface” means the physical location within the service provider’s telecommunications facilities where access to the intercepted communication or call-related information is provided;

“Minister” means the Minister of Transport and Communication or any other Minister to whom the President may from time to time assign the administration of this Act;

“monitoring centre” means a central monitoring apparatus designated to be the monitoring facility through which all the intercepted communications and call-related data of a particular interception target are forwarded to authorised persons;

“national security of Zimbabwe” includes matters relating to the existence, independence and safety of the State;

“party”, in relation to a communication, means a person whose access to the communication is or might reasonably be known by all other parties;

“warrant” means a warrant issued in terms of section 6.

(2) Any word or expression to which a meaning has been assigned in the Postal and Telecommunications Act [Chapter 12:05] shall have the same meaning when used in this Act.

PART II

CONTROL OF INTERCEPTION AND ESTABLISHMENT OF MONITORING CENTRE

3. Control of Interception

(1) Subject to subsection (2), no person shall—

- (a) intercept any communication in the course of its transmission by means of a telecommunication system or radio communication system unless—
- (i) he or she is a party to the communication; or
 - (ii) he or she has the consent of the person to whom, or the person by whom, the communication is sent; or
 - (iii) he or she is authorised by warrant;

- (b) intercept any communication in the course of its transmission through the post unless—
- (i) he or she has consent of the person to whom, or the person by whom, the communication is sent; or
 - (ii) he or she is authorised by warrant.

(2) Subsection (1) shall not apply to the *bona fide* interception of a communication for the purpose of or in connection with the provision, installation, maintenance or repair of a postal, telecommunication or radio communication service.

(3) Subject to subsections (1) and (2) any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place any communication in the course of its occurrence or transmission shall be guilty of an offence and liable to pay a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or both such fine and such imprisonment.

4. Establishment of a Monitoring centre

- (1) There shall be established a centre to be known as Monitoring of Interception of Communication Centre (MICC).
- (2) The monitoring centre shall be the sole facility through which authorised interceptions shall be effected.
- (3) The monitoring centre shall be manned, controlled and operated by designated technical experts from the agency.
- (4) The technical experts shall give technical advice to—
 - (a) authorised persons;
 - (b) to service providers;on the implementation of the interception of communications in terms of this Act.

PART III

APPLICATION FOR LAWFUL INTERCEPTION OF COMMUNICATIONS

5. Authorised persons to make an application for interception

- (1) An application for lawful interception of communications shall be made by the following persons—
 - (a) the Chief of Defence Intelligence or his or her nominee;
 - (b) the Director-General of the President's department of national security or his or her nominee;
 - (c) the Commissioner of the Zimbabwe Republic Police or his or her nominee;
 - (d) the Commissioner General of the Zimbabwe Revenue Authority or his or her nominee.
- (2) An application in terms of subsection (1) shall be made to the Minister for him or her to issue a warrant for the interception of communications.
- (3) An application in terms of subsection (1) shall indicate the following information—
 - (a) person or customer, if known, whose communication is required to be intercepted; and
 - (b) postal service provider or telecommunication service provider to whom the direction must be addressed, if applicable; and
 - (c) specify the nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and
 - (d) contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application; and
 - (e) indicate, if applicable, whether other investigative procedures have been applied and have failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be dangerous to apply in order to obtain the required evidence.

Provided that this section shall not apply to an application for the issuing of a warrant in respect of a serious offence governed by the Serious Offences Act [*Chapter 9:17*];

- (f) indicate the period for which the interception is required to be issued; and
- (g) indicate the basis for believing that communication relating to the ground on which the application is made will be obtained through the interception; and
- (h) any other information which may be required by the Minister for the Minister to make an appropriate decision.

6. Issue of warrant

- (1) An interception warrant shall be issued by the Minister to authorised persons referred to in section 5 if there are reasonable grounds for the Minister to believe that—
 - (a) a serious offence has been or is being or will probably be committed;
 - (b) the gathering of information concerning an actual threat to the national security or compelling national economic interests of the country is necessary;
 - (c) the gathering of information concerning the potential threat to safety or national security of the country is necessary;
 - (d) the interest of the country's international relations or obligation are threatened.
- (2) In the case of urgency or the existence of exceptional circumstances, an oral application may be made to the Minister by the authorised person if he or she is of the opinion that it is not reasonably practicable to make a written application, but in such case a formal application in terms of this Part shall be lodged as soon as possible with the Minister.
- (3) When circumstances so require, a warrant issued may be amended or revoked by the Minister or the Minister may issue certain directives to a service provider without the actual monitoring of a communication.

7. Scope of warrant

A warrant shall—

- (a) be valid for such period not exceeding three months as may be specified therein but may, for good cause shown, be renewed for periods not exceeding one month at a time by the Minister;
- (b) specify the name and address to which the interception shall take place or the communication facilities to be intercepted;
- (c) order the service provider to strictly comply with the technical requirements as may be required by the agency;
- (d) set out the address, number, apparatus or other factors that are to be used for identifying the communications that is to be intercepted;
- (e) set out the premises in relation to which the interception shall take place and all the necessary details relating to the interception target.

8. Non disclosure

No person shall disclose the contents of the whole or part of any communication which has been intercepted in terms of any warrant except in so far as it may be necessary for the purpose for which the warrant was issued, including proceedings in any court.

9. Evidence obtained by unlawful interception not admissible in criminal proceedings

Evidence which has been obtained by means of any interception committed in contravention of this Act shall not be admissible in any criminal proceedings except with the leave of the court and in granting or refusing such leave the court shall have regard, *inter alia*, to the circumstances in which it was obtained, its potential effect on issues of national security and the potential unfairness to the accused that might be caused by its admission.

10. Assistance by postal and telecommunications service providers

- (1) A postal or telecommunication service provider must ensure—
 - (a) that their postal or telecommunications systems are technically capable of supporting lawful interceptions at all times;
 - (b) that they install hardware and software facilities and devices to enable interception of communications;

- (c) that their services are capable of rendering real time, full time monitoring facilities for the interception of communication;
 - (d) that all associated data is provided in real-time or as soon as possible upon call termination;
 - (e) they provide one or more interfaces from which the intercepted communication shall be transmitted to the monitoring facility.
 - (f) the intercepted communications is transmitted to the monitoring facility via fixed or switched connections as may be specified by the agency;
 - (g) that they provide access to all interception subjects operating temporarily or permanently within their communications systems, and where the interception subject may be using features to divert calls to other communications service providers or terminal equipment;
 - (h) that they provide, where necessary, the capacity to implement a number of simultaneous interceptions in order—
 - (i) to allow monitoring by more than one authorised person;
 - (j) to safeguard the identities of monitoring agents and ensure the confidentiality of the investigations;
 - (i) that all interceptions are implemented in such a manner that neither the interception target nor any other unauthorised person is aware of any changes made to fulfil the interception order.
- (2) A postal or telecommunication service provider who fails to give assistance in terms of this section shall be guilty of an offence and liable to a fine not exceeding level twelve or to imprisonment for a period not exceeding three years or to both such fine and such imprisonment.

11. Duties of telecommunication service provider and customer

- (1) Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, he or she must obtain—
 - (a) the person's full names, residential address, business address or postal address and his or her identity number
 - (b) the organisation's business name and address and its registration number where applicable;
 - (c) any other information which the telecommunication service provider deems necessary for the purpose of this Act.
- (2) A telecommunication service provider must ensure that proper records are kept of information referred to in subsection (1) and where applicable, any change in such information which is brought to his or her attention.

12. Notice of disclosure of information protected by security key

- (1) If an authorised person believes on reasonable grounds—
 - (a) that a key to the protected information is in the possession of any person;
 - (b) that the imposition of a disclosure requirement in respect of the protected information is—
 - (i) necessary in the interests of national security;
 - (ii) necessary for the purpose of preventing and detecting crime; or
 - (iii) in the interests of the economic well-being of Zimbabwe
- (c) that the imposition of such a requirement is proportionate to what is sort to be achieved by its imposition;
- (d) that it is reasonably impracticable for the authorised person to obtain possession of the protected information in an intelligible form without giving the notice under this section;

the authorised person may by notice to the person whom he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

- (2) A notice under this section imposing a disclosure requirement in respect of any protected information must—
 - (a) be in writing;
 - (b) describe the protected information to which the notice relates;
 - (c) relate to matters referred to in subsection (1);
 - (d) specify the reasonable time by which the notice is to be complied with; and
 - (e) set out the disclosure that is required by the notice and the form and manner in which it is to be made.
- (3) A notice under this section shall not require the making of any disclosure to any person other than—
 - (a) a person giving the notice; or
 - (b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.
- (4) A person to whom a notice has been given in terms of this section and who is in possession of both the protected information and the key thereto—
 - (a) may use any key in his or her possession to provide access to the information;
 - (b) must, in providing such information, make a disclosure of the information in an intelligible form.
- (5) If, a person to whom a notice has been given, is in possession of different keys, or combinations of keys to the protected information—
 - (a) it shall not be necessary for purposes of complying with the notice requirement, for the person given notice to disclose any keys in addition to those the disclosure of which, alone, is sufficient to enable the authorised person to whom they are disclosed to obtain access to the protected information and to put it in an intelligible form;
 - (b) the person given notice may select which of the keys or combination of keys, to disclose for purposes of complying with the requirements.
- (6) If a person to whom a notice has been given—
 - (a) has been in the possession of the keys to the protected information, but is no longer in possession thereof;
 - (b) is in possession of any information that would facilitate the obtaining or discovery of the keys to protected information;
he or she must disclose all such information as is in his or her possession to the authorised person.
- (7) An authorised person to whom a key has been disclosed under this section—
 - (a) shall use the key only in respect of the protected information, and in the manner and for the purposes, specified in the notice; and
 - (b) must, on or before the expiry of the period or extended period for which the notice has been issued, destroy all records of the disclosed key if, in the opinion of the authorised person—
 - (i) no criminal proceedings or civil proceedings will be instituted in connection with such records; or
 - (ii) such records will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes of order of court.
- (8) A person who fails to make the disclosure as required by the notice shall be guilty of an offence and liable to a fine not exceeding twenty million dollars or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

13. Interception capability of telecommunication service

- (1) Notwithstanding any other law, a telecommunication service provider shall—
 - (a) provide a telecommunication service which has the capability to be intercepted; and
 - (b) store communication-related information.
- (2) The Postal and Telecommunication Authority shall, after consultation with the Minister, within two months after the fixed date, issue a directive to telecommunication service providers determining—
 - (a) the manner in which effect is to be given to subsection (1) by the telecommunication service provider;
 - (b) security, technical and functional requirements of the facilities and devices to be acquired by the telecommunication service provider to enable—
 - (i) the interception of communication in terms of this Act;
 - (ii) the storing of communication-related information;
 - (c) the period for which compliance with such directive must be fulfilled.
- (3) A directive referred to in subsection (2) must prescribe the—
 - (a) capacity needed for interception purposes;
 - (b) technical requirement of the systems to be used;
 - (c) connectivity with the interception monitoring centre;
 - (d) manner of routing information to the interception monitoring centre;
 - (e) any other relevant matter which the Authority deems necessary or expedient.
- (4) A telecommunication service provider shall, at his or her own expense acquire the facilities and devices determined in a directive issued in terms of subsection (2).
- (5) Any cost incurred by a telecommunication service provider under this Act in—
 - (a) enabling—
 - (i) a telecommunication service to be intercepted; and
 - (ii) communication related information to be stored; and
 - (b) complying with section (10);must be borne by that telecommunication service provider.

14. Compensation payable to postal service provider or telecommunication service provider or protected information key holder

- (1) The Minister, after consultation with the Authority, shall by notice in the *Gazette* prescribe—
 - (a) the forms of assistance in the execution of a directive for which a postal service provider, telecommunications service provider or protected information key holder, must be compensated; and
 - (b) reasonable tariffs of compensation payable to a postal service provider, telecommunication service provider or protected information key holder for providing such prescribed forms of the assistance.
- (2) The tariffs prescribed under subsection (1)(b)—
 - (a) may differ in respect of different categories of postal service providers, telecommunication service providers or protected information key holders;
 - (b) must be uniform in respect of each postal service provider, telecommunication service provider or protected information key holder falling within the same category.
- (3) The forms of assistance referred to in this section must include, in the case of—
 - (a) a telecommunication service provider, the making available of a facility, device or telecommunication system; and
 - (b) a protected information key holder—
 - (i) the disclosure of the key; and
 - (ii) the provision assistance

- (4) The compensation payable to postal service provider, telecommunication service provider or protected information key holder shall only be for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance in subsection (1).

PART IV

GENERAL PROHIBITIONS AND EXEMPTIONS

15. General prohibitions and exemptions

- (1) No person may disclose any information which he or she obtained in the exercise of his or her powers or the performance of his or her duties in terms of the Act except—
 - (a) to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;
 - (b) if he or she is a person who of necessity supplies it in the performance of his or her functions in terms of this Act;
 - (c) information which is required in terms of any law or as evidence in any court of law.
- (2) No—
 - (a) postal service provider, telecommunication service provider or protected information key holder may disclose any information which he or she obtained in the exercise of his or her powers or the performance of his or her duties in terms of this Act; or
 - (b) employee of a postal service provider, telecommunication service provider or protected information key holder may disclose any information which he or she obtained in the course of his or her employment and which is connected with the exercise of any power or the performance of any duty in terms of this Act.
- (3) Any person who discloses any information in terms of subsection (1) shall be guilty of an offence and liable to a fine of not exceeding ten million dollars or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

16. Disclosure of information by authorised person

Notwithstanding section 15, any authorised person who executes an interception or assists with the execution thereof and who has obtained knowledge of the contents of any communication intercepted may disclose such contents to the extent that such disclosure is necessary for the proper performance of the official duties of the authorised person.

17. Disposal of intercept product

The authorised person shall destroy beyond any retrievable proportions as soon as possible after use any intercepted product.

18. Application for a detention and examination order

- (1) A person authorised in terms of section 5 shall, if he or she suspects on reasonable grounds that a postal article in the custody of a postal licensee—
 - (a) contains anything in respect of which an offence or attempted offence is being committed; or
 - (b) contains anything that will afford evidence of the commission of an offence; or
 - (c) is being sent to further the commission of an offence;

may apply to the Minister for a detention order to detain the postal article for the purpose of examination.

- (2) If the Minister, by written order to the authorised person, certifies that it is necessary in the interests of defence, public safety or public order for a postal article in the

postal licensee's custody to be detained and additionally, or alternatively, opened and examined, the postal licensee shall forth with comply with the order.

- (3) Section 5 shall apply with necessary changes to the information required to be furnished to the Minister before a detention order is issued.

19. Examination and accountability for detained postal articles

- (1) On an appointed day the authorised person shall, in the presence of the postal licensee or his or her nominee, examine the detained postal article.
- (2) If, on examination of a postal article in terms of subsection (1)—
 - (a) the suspicion that gave rise to its examination is substantiated, the postal article may be detained for the purposes of prosecution or destroyed or dealt with in such other manner as may be prescribed;
 - (b) the suspicion that gave rise to its examination is not substantiated, the postal article shall be delivered to the person to whom it is addressed or to his or her representative on payment of any postage payable thereon.

20. Appeals

- (1) Any person who is aggrieved by a decision made by the Authority, authorised person or agency may appeal to the Minister within fourteen days after being notified of the decision, and the Minister may confirm, vary or set aside the decision appealed against or make such other order in the matter as he or she thinks appropriate.
- (2) Any person who is aggrieved by a decision made by the Minister in terms of this Act may appeal against it to the Administrative Court within one month after being notified of the decision.
- (3) The Administrative court may in any appeal confirm, vary or set aside the decision or action appealed against and may make such order, whether as to costs or otherwise, the court thinks just.

21. Regulations

The Minister may make regulations providing for all matters which by this Act are required or permitted to be prescribed or which, in his or her opinion, are necessary or convenient to be prescribed for carrying out or giving effect to this Act.