WORKING DOCUMENT
DRAFT 6
(As on 03/09/2002)
REPUBLIC OF SOUTH AFRICA

THE REGULATION OF INTERCEPTION OF COMMUNICATIONS BILL

As presented by the Portfolio Committee on Justice and Constitutional Development (National Assembly), after consideration of the Interception and Monitoring Bill [B 50—2001]) (The English text is the official text of the Bill)

(MINISTER FOR JUSTICE AND CONSTITUTIONAL DEVELOPMENT)

[B 50 - 2001]

Workdoc9

GENERAL EXPLANATORY NOTE:

[xxxxx] Words in bold type in square brackets and which are shaded indicate omissions from the previous Working document (Draft 5), as proposed during deliberations on, and in comment received in respect of, that Working document.

[xxxxxx] Words underlined with a solid line and which are shaded indicate new insertions in the previous Working document (Draft 5), as proposed during deliberations on, and in comment received in respect of, that Working document.

FURTHER NOTE: The changes proposed to the long title and clauses 23, 32 to 37 and 51 during the discussion of the previous Working document (Draft 5) have not yet been effected to the long title and those clauses as they appear in this Working document.

BILL

To regulate the interception **[and monitoring]** of certain communications; to provide for the interception of postal articles and communications **[and for the monitoring of communications in the case of a serious offence or if the security or other compelling national interests of the Republic are threatened]** under certain circumstances; to prohibit the provision of certain telecommunication services which do not have the capacity to be **[monitored]** intercepted; to regulate authorised telecommunications **[monitoring]** interception; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

ARRANGEMENT OF SECTIONS

CHAPTER 1

INTRODUCTORY PROVISIONS

Definitions and interpretation

1. In this Act, unless the context otherwise indicates—

"Agency" means the Agency as defined in section 1 of the Intelligence Services Act;

"applicant" means—

a. an officer referred to in section 33 of the South African Police Service Act, if the officer concerned obtained in writing the approval in advance of another officer in the Police Service with at least the rank of assistant-commissioner and who has been authorised in writing by the National Commissioner of the Police Service to grant such approval;

b. an officer as defined in section 1 of the Defence Act, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of major-general who must be authorised in writing by the Chief of the Defence Force to grant such approval;

c. a member as defined in section 1 of the Intelligence Services Act, if the member concerned obtained in writing the approval in advance of another member of the Agency or the Service, as the case may be, holding a post of at least general manager;

d. the head of the Directorate or an Investigating Director authorised thereto in writing by the head of the Directorate; **[or]**

e. the National Director or a Deputy National Director authorised thereto in writing by the National Director; or

f. a member of the Independent Complaints Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director, appointed in terms of section 51 of the South African Police Service Act;

"archived communication-related direction" means a direction issued under section 18(3)(a) or 19(3) in terms of which a telecommunication service provider is directed to provide archived communication-related information in respect of a customer**[, and includes an oral archived communication-related direction issued under section 21(7)]**;

"archived communication-related information" means any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)(b) for the period determined in a directive referred to in section 30(2)(a), beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;

"authorised person" means any—

a. law enforcement officer who may, in terms of section 26(1)(a)(i), execute a direction; or

b. law enforcement officer or other person who may, in terms of section 26(1)**[(b)]**(a)(ii), assist with the execution of a direction;

"Authority" means the Independent Communications Authority of South Africa established by section 3 of the Independent Communications Authority of South Africa Act, 2000 (Act No. 13 of 2000);

"business" means any business activity conducted by any person, including activities of any**[—**

a. **department of state or administration in the national, provincial or local sphere of government; or**

b. **other functionary or institution exercising a public power or performing a public function in terms of the Constitution or any legislation]** private or public body;

"cellular phone" means any fixed or mobile cellular apparatus or terminal which is capable of connection to a cellular telecommunication system and which is used by a customer to transmit or receive indirect communications over such telecommunication system;

"communication" includes both a direct communication and an indirect communication;

"communication-related information" means any information relating to an indirect communication which is available in the records of a telecommunication service provider and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunications system;

"Constitution" means the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996);

"contents", when used with respect to any communication, includes any information concerning the substance, purport or meaning of that communication;

"customer" means any person—

(a) to whom a telecommunication service provider provides a telecommunication service; or
(b) who has entered into a contract with a telecommunication service provider for the provision of a telecommunication service, including a pre-paid telecommunication service;

"decryption assistance" means to—

a. allow access, to the extent possible, to encrypted information; or

b. facilitate the putting of encrypted information into an intelligible form;

"decryption direction" means a direction issued under section 21(3) in terms of which a decryption key holder is directed to—

a. disclose a decryption key; or

b. provide decryption assistance in respect of encrypted information,

and includes an oral decryption direction issued under section 23(7);

"decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to—

a. allow access to encrypted information; or

b. facilitate the putting of encrypted information into an intelligible form;

"decryption key holder" means any person who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to indirect communications;

"Defence Act" means the Defence Act, 1957 (Act No. 44 of 1957);

"Defence Force" means the defence force referred to in section 199(2) of the Constitution **[of the Republic of South Africa, 1996 (Act No. 108 of 1996)]**;

"direct communication" means—

a. an oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or

b. an utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication;

"direction" means any interception direction, archived communication-related direction, **[supplementary direction,]** real-time communication-related direction or decryption direction issued under this Act, and includes an oral direction issued under section 23(7), but, for purposes of section 20, excludes an archived communication-related direction;

"Director" means the Director of Interception Centres;

"Directorate" means the Directorate of Special Operations referred to in section 1 of the National Prosecuting Authority Act;

"encrypted information" means any electronic data which, without the decryption key to that data—

a. cannot, or cannot readily, be accessed; or

b. cannot, or cannot readily, be put into an intelligible form;

"entry warrant" means a warrant issued under section 22(3) and which authorises entry upon any premises for purposes of—

a. intercepting a postal article or communication on the premises; or

b. installing and maintaining an interception device on, and removing an interception device from, the premises, and includes an oral entry warrant issued under section 23(7);

"fixed date" means the date of commencement of this Act;

"Fund" means the **[Interception]** Internet Service Providers Assistance Fund established by section 38(1);

"Identification Act" means the Identification Act, 1997 (Act No. 68 of 1997);

"identification document" means, in the case of a person who is—

a. a South African citizen or is lawfully and permanently resident in the Republic and has attained the age of 16 years—

i. an identity card or temporary identity certificate as defined in the Identification Act;

ii. a green, bar-coded identity document issued in accordance with the Identification Act, 1986 (Act No. 72 of 1986), until such identity document is replaced by an identity card as contemplated in section 25 of the Identification Act; or

iii. a South African passport as defined in the South African Passports and Travel Documents Act, 1994 (Act No. 4 of 1994);

b. a South African citizen or is lawfully and permanently resident in the Republic and has not attained the age of 16 years, a birth certificate referred to in section 13 of the Identification Act; and

c. not a South African citizen or is not permanently resident in the Republic—

i. a travel document as defined in the South African Passports and Travel Documents Act, 1994 ; or

ii. a passport or travel document as contemplated in paragraphs (b), (c) and (d) of the definition of "passport" in the Immigration Act, 2002 (Act No. 13 of 2002);

"Independent Complaints Directorate" means the Independent Complaints Directorate established by section 50(1) of the South African Police Service Act;

"indirect communication" means the transfer of information, including a message or any part of a message, whether—

a. in the form of—

i. speech, music or other sounds;

ii. data;

iii. text;

iv. visual images, whether animated or not; or

v. signals; or

b. in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system;

"Intelligence Services Act" means the Intelligence Services Act, 1994 (Act No. 38 of 1994);

"intelligible form" means the form in which electronic data was before an encryption or similar process was applied to it;

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

a. monitoring of any such communication by means of a monitoring device;

b. viewing, examination or inspection of the contents of any indirect communication; and

c. diversion of any indirect communication from its intended destination to any other destination, and "interception" has a corresponding meaning;

"interception centre" means an interception centre established by section 32(1);

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

a. any instrument, device, equipment or apparatus, or any component thereof—

i. furnished to the customer by a telecommunication service provider in the ordinary course of his or her business and being used by the customer in the ordinary course of his or her business;

ii. furnished by such customer for connection to the facilities of such telecommunication service and used in the ordinary course of his or her business;

iii. being used by a telecommunication service provider in the ordinary course of his or her business; or

iv. *{being used by a law enforcement officer in the ordinary course of exercising his or her powers or performing his or her duties, which powers or duties do not involve the interception of communications; or}*

b. a hearing aid or similar device being used to correct below normal hearing to not better than normal, and a reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

"interception direction" means a direction issued under section 16(4) or 18(3)(a) and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued

under section 23(7);

"Internet" means the international computer network known by that name;

"Internet service provider" means any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with a telecommunication service licence issued to the first-mentioned person under Chapter V of the Telecommunications Act;

"designated judge" means any judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001), **[and]** or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act;

"law enforcement officer" means any—

a. member of the Police Service;

b. member of the Defence Force, excluding a member of a visiting force**[, as defined in section 1 of the Defence Act]**;

c. member of the Agency or the Service;

d. member of the Directorate; or

e. other member of the prosecuting authority;

"listed equipment" means any equipment declared to be listed equipment under section 44(1), and includes any component of such equipment;

"Minister" means the Cabinet member responsible for the administration of justice;

"**[monitoring]** monitor" includes to listen to or record communications by means of a monitoring device, and "monitoring" has a corresponding meaning;

"monitoring device" means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication;

"National Director" means the National Director of Public Prosecutions contemplated in section 179(1)(a) of the Constitution **[of the Republic of South Africa, 1996 (Act No. 108 of 1996)]**;

"National Prosecuting Authority Act" means the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);

"Office" means the Office for Interception Centres established by section 33(1);

"oral direction" means any direction issued under section 23(7);

"oral entry warrant" means an entry warrant issued under section 23(7);

["organised fashion", for purposes of paragraph (b)(ii) of the definition of "serious offence" includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that has the same or similar intents, results, accomplices, victims or methods of commission, or otherwise are related by distinguishing characteristics;]

"party to the communication", for purposes of—

a. sections 4 and 6(1)(a)(i), means, in the case of—

   i. a direct communication, any person—

      (aa) participating in such direct communication or to whom such direct communication is directed; or

      (bb) in whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is specifically directed to him or her; or

   ii. an indirect communication—

      (aa) the sender or the recipient or intended recipient of such indirect communication;

      (bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients; or

      (cc) any other person who, at the time of the occurrence of the indirect communication, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication; and

b. sections 5 and 6(1)(a)(ii), means, in the case of—

i. a direct communication, any person participating in such direct communication or to whom such direct communication is directed; or

ii. an indirect communication—

(aa) the sender or the recipient or intended recipient of such indirect communication; or

(bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients;

"Police Service" means the South African Police Service established by section 5(1) of the South African Police Service Act;

"postal article" means any postal article as defined in the Postal Services Act;

"postal service" means a postal service as defined in the Postal Services Act, and includes—

a. any private postal service; and

b. any service which is offered or provided as a service of which, or one of the main purposes of which, is to make available, or to facilitate, a means of transmission from one place to another place of postal articles containing indirect communications;

"Postal Services Act" means the Postal Services Act, 1998 (Act No. 124 of 1998);

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

{"pre-paid telecommunication service" means a mobile cellular telecommunication service in respect of which—

a. a service provider provides the service to a customer without the customer concerned having to enter into a contract with the service provider for the provision of that service to the customer;

b. the customer pays for the provision of the service before it is used; and

c. no other person, body or organisation, including another service provider, gives the customer an account for the provision of the service after it has been used;}

"premises" includes any land, building, structure, vehicle, ship, boat, vessel, aircraft or container;

"Prevention of Organised Crime Act" means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);

"private body" means—

a. a natural person who carries on any trade, business or profession, but only in such capacity;

b. a partnership which carries on any trade, business or profession; or

c. any juristic person,

but excludes a public body;

"prosecuting authority" means the single national prosecuting authority established in terms of section 179 of the Constitution;

"public body" means—

a. any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

b. any other functionary or institution when—

i. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

ii. exercising a public power or performing a public function in terms of any legislation;

"real-time communication-related direction" means a direction issued under section 17(4) or 18(3) in terms of which a telecommunication service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available, and includes an oral real-time communication-related direction issued under section 23(7);

"real-time communication-related information" means communication-related information which is immediately available to a telecommunication service provider—

a. before, during, or for a period of 90 days after, the transmission of an indirect communication; and

b. in a manner that allows the communication-related information to be associated with the indirect communication to which it relates;

"relevant Ministers" means the—

a. Minister of Communications;

b. Minister of Defence;

c. Minister of Intelligence; and

d. Minister for Safety and Security;

"serious offence" means—

a. any offence mentioned in the Schedule; or

b. any offence that is allegedly being or has allegedly been or will probably be committed by a person, group of persons or syndicate—

(i) acting in an organised fashion which includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that has the same or similar intents, results, accomplices, victims or methods of commission, or otherwise are related by distinguishing characteristics;

[(i)](ii) acting in the execution or furtherance of a common purpose or conspiracy; or

[(ii) acting in an organised fashion;]

(iii) which could result in substantial financial gain for the person, group of persons or syndicate committing the offence**[; or**

(iv) which may cause substantial *{and irreparable}* harm to the international relations or economy of the Republic],

including any conspiracy, incitement or attempt to commit any of the above-mentioned offences;

"Service" means the Service as defined in section 1 of the Intelligence Services Act;

"SIM-card" means the Subscriber Identity Module which is an independent, electronically activated device designed for use in conjunction with a cellular phone to enable the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to identify the particular Subscriber Identity Module and its installed information;

"South African Police Service Act" means the South African Police Service Act, 1995 (Act No. 68 of 1995);

["supplementary direction" means a direction issued under section 16(4) in terms of which a telecommunication service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available, and includes an oral supplementary direction issued under section 21(7)];

"system controller" **[means, in relation to a particular telecommunication system, a person with a right to control its operation or use]** of, or in relation to—

a. a private body, means in the case of a—

i. natural person, that natural person or any person duly authorised by that natural person;

ii. partnership, any partner of the partnership or any person duly authorised by the partnership; or

iii. juristic person—

(aa) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or

(bb) the person who is acting as such or any person duly authorised by such acting person; and

b. a public body, means in the case of—

i. a national department, provincial administration or organisational component—

(aa) mentioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person who is acting as such; or

(bb) not so mentioned, the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or organisational component, respectively, or the person who is acting as such;

ii. a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998), or the person who is acting as such; or

iii. any other public body, the chief executive officer, or equivalent officer, of that public body or the person who is acting as such;

"Telecommunications Act" means the Telecommunications Act, 1996 (Act No. 103 of 1996);

"telecommunication service" means any telecommunication service as defined in the Telecommunications Act;

"telecommunication service provider" means any—

a. person who provides a telecommunication service under and in accordance with a telecommunication service licence issued to such person under Chapter V of the Telecommunications Act, and includes any person who provides—

i. a local access telecommunication service, public pay-telephone service, value-added network service or private telecommunication network as defined in the Telecommunications Act; or

ii. any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act; and

b. Internet service provider;

"telecommunication system" means a telecommunication system as defined in the Telecommunications Act.

(2) For purposes of this Act—

a. the interception of a communication takes place in the Republic if, and only if, the interception is effected by conduct within the Republic and the communication is either intercepted, in the case of—

i. a direct communication, in the course of its occurrence; or

ii. an indirect communication, in the course of its transmission by means of a postal service or telecommunication system, as the case may be; and

b. the **[times while]** time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.

(3) A reference in this Act to the interception of a communication does not include a reference to the interception of any indirect communication which is broadcast or transmitted **[/broadcast]** for general reception.

CHAPTER 2

PROHIBITION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF ARCHIVED OR REAL-TIME COMMUNICATION-RELATED INFORMATION AND EXCEPTIONS

Part 1

Prohibition of interception of communications and **[provision of archived or real-time communication-related information]** exceptions

Prohibition of interception of communication

2. Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.

Interception of communication under interception direction

3. Subject to this Act, any—

a. authorised person who executes an interception direction or assists with the execution thereof, may intercept any communication; and

b. postal service provider to whom an interception direction is addressed, may intercept any indirect communication, to which that interception direction relates.

Interception of communication by party to communication

4. (1) Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.

(2) Any law enforcement officer may intercept any communication if he or she is—

a. a party to the communication; and

b. satisfied that there are reasonable grounds to believe that the interception of a communication of another party to the communication is necessary on a ground referred to in section 16(5)(a), unless such communication is intercepted by such law

enforcement officer for purposes of committing an offence**[; and**

c. of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application in terms of section 14(1) or 21(1) for the issuing of an interception direction or an oral interception direction.

(3) As soon as practicable after steps relating to the interception of a communication under subsection (2) have been taken, the law enforcement officer who is involved in the interception of the communication concerned must cause the relevant applicant to make an application in terms of section 14(1) for the issuing of an interception direction in respect of that communication.

(4) Subsection (3) does not apply if steps have been taken under subsection (2) to intercept a communication, or cause it to be intercepted, and the taking of those steps have ceased before it is practicable for an application to be made in terms of section 14(1) for the issuing of an interception direction in respect of that communication.

(5) If a judge, after considering an application made to him or her in relation to the interception of a communication under subsection (2), refuses to issue an interception direction—

a. the applicant concerned must ensure that no further steps are taken to intercept the communication concerned or cause it to be intercepted; and

b. section 23(6) applies, with the necessary changes, in respect of any communication intercepted under subsection (2).]

Interception of communication with consent of party to communication

5. (1) Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.

(2) Any law enforcement officer may intercept any communication if—

a. one of the parties to the communication has given prior consent in writing to such interception;

b. he or she is satisfied that there are reasonable grounds to believe that the party who has given consent as contemplated in paragraph (a) will—

1. participate in a direct communication or that a direct communication will be directed to him or her; or

2. send or receive an indirect communication; and

c. the interception of such direct or indirect communication is necessary on a ground referred to in section 16(5)(a),

unless such communication is intercepted by such law enforcement officer for purposes of committing an offence**[; and**

(c) he or she is of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application in terms of section 14(1) or 21(1) for the issuing of an interception direction or an oral interception direction.

(3) Section 6(3), (4) and (5) applies, with the necessary changes, in respect of the interception of a communication under subsection (2)].

Interception of communication or obtaining of real-time communication-related information to prevent serious bodily harm [or serious damage to property]

6. (1) **[Subject to section 45(3), any]** Any law enforcement officer may, **[intercept any communication]** if—

a. (i) he or she is a party to the communication; **[or]**

(ii) one of the parties to the communication has given prior consent **[in writing]** to such interception; or

[(b)] (iii) he or she is satisfied that there are reasonable grounds to believe that another party to the communication has—

[(i)] (aa) caused, or may cause, the infliction of serious bodily harm to another person **[or serious damage to property of another person]**;

[(ii)] (bb) threatens or has threatened to cause the infliction of serious bodily harm to another person **[or serious damage to property of another person]**; or

[(iii)] (cc) threatens or has threatened to take his or her own life or to perform an act which would or may endanger his or her own life or would or may cause the infliction of serious bodily harm to himself or herself;

[(c)](b) he or she is of the opinion that because of the urgency of the need to intercept the communication or to obtain real-time communication-related information, it is not reasonably practicable to make an application in terms of section 16(1), 17(1) or 23(1) for the issuing of an interception direction or a real-time communication-related direction or an oral interception direction or oral real-time

communication-related direction; and

[(d)](c) the sole purpose of the interception or the obtaining of the real-time communication-related information is to prevent such bodily harm **[or damage to the property]**, intercept any communication or may orally request a telecommunication service provider to route duplicate signals of indirect communications or the real-time communication-related information specified in that request to an interception centre designated therein or to provide him or her with the real-time communication-related information specified in that request.

(2) A telecommunication service provider must, upon receipt of a request made to him or her in terms of subsection (1)—

a. route the duplicate signals of the indirect communications concerned to the designated interception centre;

b. route the real-time communication-related information concerned, as soon as practicable after it became available, to the designated interception centre; or

c. provide the real-time communication-related information sconcerned, as soon as practicable after it became available, to the law enforcement officer concerned.

(3) The law enforcement officer who made a request under subsection (1) must as soon as practicable after making that request, furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request.

(4) The law enforcement officer who intercepts a communication or obtains real-time communication-related information under subsection (1) or (2) must, as soon as practicable after the interception of the communication or the obtaining of the real-time communication-related information concerned, submit to a designated judge—

(a) a copy of the written confirmation referred to in subsection (3);

(b) an affidavit setting forth the results and information obtained from that interception or real-time communication-related information; and

[(b)](c) any recording of the communication that has been obtained by means of that interception, any full or partial transcript of the recording and any notes made by that law enforcement officer of the communication or real-time communication-related information if nothing in the communication or real-time communication-related information suggests that bodily harm, attempted bodily harm or threatened bodily harm has been caused or is likely to be caused.

(5) A telecommunication service provider who, in terms of subsection (2), has—

a. routed duplicate signals of indirect communications to the designated interception centre;

b. routed real-time communication-related information to the designated interception centre; or

c. provided real-time communication-related information to the law enforcement officer concerned,

must, as soon as practicable thereafter, submit an affidavit to a designated judge setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results obtained from such steps.

(6) A designated judge must**[, as soon as practicable after receipt of]** keep all written confirmations and affidavits and any recordings, transcripts or notes submitted to him or her in terms of subsections **[(2)]** (4) and (5), **[destroy such recording, transcript or notes]** or cause it to be **[destroyed in his or her presence]** kept, for a period of at least five years.

Interception of communication for purposes of determining location in case of emergency

7. (1) In circumstances where—

a. a person is a party to a communication;

b. that person, as a result of information received from another party to the communication (in this section referred to as the "sender"), has reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person, whether or not the sender, is being endangered or that he or she is dying or is being or has been seriously injured or that his or her life is likely to be endangered or that he or she is likely to die or to be seriously injured; and

c. the location of the sender is unknown to that person,

the person referred to in paragraph (a) may, if he or she is—

i. a law enforcement officer, and if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to—

(aa) intercept any communication to or from the sender for purposes of determining his or her location; or

(bb) determine the location of the sender in any other manner which the telecommunication service provider deems appropriate; or

ii. not a law enforcement officer, inform, or cause another person to inform, any law enforcement officer of the matters referred to in paragraphs (a), (b) and (c).

(2) A law enforcement officer who has been informed as contemplated in subsection (1)(ii), may, if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to act as contemplated in subsection (1)(i)(aa) or (bb).

(3) A telecommunication service provider **[may]** must, upon receipt of a request made to him or her in terms of subsection (1)(i) or (2)—

a. intercept any communication to or from the sender for purposes of determining his or her location; or

b. determine the location of the sender in any other manner which the telecommunication service provider deems appropriate,

and if the location of the sender has been so determined, the telecommunication service provider concerned must, as soon as practicable after determining that location, provide the law enforcement officer who made the request with the location of the sender and any other information obtained from that interception which, in the opinion of the telecommunication service provider concerned, is likely to be of assistance in dealing with the emergency.

(4) The law enforcement officer who made a request under subsection (1)(i) or (2) must—

a. as soon as practicable after making that request, furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request;

b. as soon as practicable after making that request, furnish a designated judge with a copy of such written confirmation; and

c. if the location of the sender and any other information has been provided to him or her in terms of subsection (3), as soon as possible after receipt thereof, submit to a designated judge an affidavit setting forth the results and information obtained from that interception.

(5) A telecommunication service provider who has taken any of the steps contemplated in subsection (3), must, as soon as practicable thereafter, submit an affidavit to a designated judge setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results obtained from such steps.

(6) A designated judge must keep **[a record of]** all written confirmations and **[information]** affidavits submitted to him or her in terms of subsections (4)(b) and (c) and (5), or cause it to be kept, for a period of at least five years.

Interception of communication for purposes of installation or maintenance of equipment, facilities or devices

8. (1) Any person who is lawfully engaged in duties relating to—

a. the installation or connection of any equipment, facility or device used, or intended to be used, in connection with a telecommunication service;

b. the operation or maintenance of a telecommunication system; or

c. the installation, connection or maintenance of any interception device used, or intended to be used, for the interception of a communication under an interception direction,

may, in the ordinary course of the performance of those duties, intercept a communication where it is reasonably necessary for that person to intercept the communication in order to perform those duties effectively.

{(2) Any information obtained by means of the interception of a communication as contemplated in subsection (1) may only be ***[—***

(a)] *used for purposes of performing the duties referred to in that subsection}* **[;**

(b) disclosed for purposes of reporting the suspected commission of any offence by any person of which the person intercepting the communication concerned becomes aware during such interception, to the Director of Public Prosecutions having jurisdiction in the area in which such offence has been or is being or will probably be committed; or

(c) disclosed as contemplated in section 40(1)(d)].

(3) Any person who intercepted a communication as contemplated in subsection (1) must, as soon as practicable thereafter, submit an affidavit to a designated judge setting forth the information obtained by means of that interception

(4) A designated judge must keep all affidavits submitted to him or her in terms of subsection (3), or cause it to be kept, for a period of at least five years.

Interception of indirect communication in connection with carrying on of business

9. (1) Any person may, in the course of the carrying on of any business, intercept any indirect communication—

a. by means of which a transaction is entered into in the course of that business;

b. which otherwise relates to that business; or

c. which otherwise takes place in the course of the carrying on of that business,

in the course of its transmission over a telecommunication system, if such interception is effected by, or with the express or implied consent of, the system controller.

(2) A person may only intercept an indirect communication in terms of subsection (1)—

a. for purposes of—

i. monitoring or keeping a record of indirect communications—

(aa) in order to establish the existence of facts;

(bb) in the interests of the public health or safety or national security of the Republic;

(cc) for purposes of preventing the commission of a serious offence;

(dd) for purposes of investigating or detecting the unauthorised use of that or any other telecommunication system; or

(ee) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or

ii. monitoring indirect communications—

(aa) for purposes of determining whether they are communications relevant to the business of the system controller as contemplated in subsection (1)(a) or (b); or

(bb) made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose;

a. if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and

b. if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system.

Interception of communications authorised by certain other Acts

10. (1) Any communication may, in the course of its occurrence or transmission, be intercepted in any prison as defined in section 1 of the Correctional Services Act, 1998 (Act No. 111 of 1998), if such interception takes place in the exercise of any power conferred by or under, and in accordance with, any regulations made under that Act.

(2) If any regulations referred to in subsection (1)—

a. were made prior to the fixed date, the Minister of Correctional Services must within one month after the fixed date, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within one month after the commencement of its next ensuing ordinary session, submit a copy of those regulations to Parliament; or

b. are made after the fixed date, the Minister of Correctional Services must, before the publication thereof in the *Gazette*, submit those regulations in draft form to Parliament.

[OPTION 2

(2) If any regulations referred to in subsection (1)—

a. were made prior to the fixed date, the Minister of Correctional Services (in this section referred to as the "Minister") must within one month after the fixed date, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within one month after the commencement of its next ensuing ordinary session, table a copy of those regulations, as originally published in the Gazette, in Parliament for approval; or

b. made after the fixed date, the Minister must, before the publication thereof in the Gazette, table those regulations in draft form in Parliament for approval.

(3) Parliament may reject the regulations tabled in terms of subsection (2) within two months after they have been tabled.

(4) If Parliament rejects any regulations, the Minister must, in the case of regulations tabled in terms of—

a. subsection (2)(a)—

(i) repeal them; or
(ii) table amended regulations in draft form in Parliament,

within two months of the rejection if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within two months after the commencement of its next ensuing ordinary session, failing which the regulations become invalid; or

b. subsection (2)(b), table amended regulations in draft form in Parliament.

(5) If the Minister tables amended regulations and Parliament—

a. approves the amended regulations, the Minister must publish them in the Gazette within one month of Parliament's approval; or

b. rejects the amended regulations, subsection (4) and this subsection apply.

(6) If the Minister complies with subsection (4)(a)(ii), the regulations as originally published in the Gazette continue to apply until amended regulations are approved by Parliament and published by the Minister in the Gazette.]

Monitoring of signal and radio frequency for purposes of managing radio frequency spectrum

11. (1) Any person appointed as an inspector in terms of section 98 of the Telecommunications Act and who is lawfully engaged in performing the functions of the Authority relating to the management of the radio frequency spectrum, as contemplated in section 28(1) of that Act, may, in the ordinary course of the performance of those functions, monitor a signal or radio frequency relating to an indirect communication which is transmitted over a radio, where it is reasonably necessary for that employee to monitor that signal or radio frequency for purposes of identifying, isolating or preventing an unauthorised or interfering use of a frequency or of a transmission.

{(2) Any information obtained by means of the monitoring of an indirect communication as contemplated in subsection (1) may only be used for the purposes referred to in that subsection.}

Part 2

Prohibition of provision of archived or real-time communication-related information and exceptions [to prohibitions]

Prohibition of provision of archived or real-time communication-related information

12. Subject to this Act, no telecommunication service provider or employee of a telecommunication service provider may provide or attempt to provide any archived or real-time communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such archived or real-time communication-related information relates.

Provision of archived or real-time communication-related information under archived communication-related direction[, supplementary direction] or real-time communication-related direction

13. Subject to this Act, any telecommunication service provider to whom an archived communication-related direction[, supplementary direction] or real-time communication-related direction is addressed, may provide any archived or real-time communication-related information to which that archived communication-related direction[, supplementary direction] or real-time communication-related direction relates.

Provision of archived or real-time communication-related information upon authorisation by customer

14. Any telecommunication service provider may, upon the written authorisation given by his or her customer on each occasion, and subject to the conditions determined by the customer concerned, [by his or her customer in each case,] provide to any person specified by that customer archived or real-time communication-related information which relates to the customer concerned.

Availability of other procedures for obtaining archived or real-time communication-related information

15. (1) Subject to subsection (2), the availability of the procedures in respect of the provision of archived or real-time communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.

(2) Any archived or real-time communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis.

CHAPTER 3

APPLICATIONS FOR, AND ISSUING OF, DIRECTIONS AND ENTRY WARRANTS

Application for, and issuing of, interception direction

16. (1) An applicant may apply to a designated judge for the issuing of an interception direction.

(2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must—

a. indicate the identity of the—

i. applicant and, if known and appropriate, the identity of the law enforcement officer who will execute the interception direction;

ii. person or customer, if known, whose communication is required to be intercepted; and

iii. postal service provider or telecommunication service provider to whom the direction must be addressed, if applicable;

b. specify the ground referred to in subsection (5)(a) on which the application is made;

c. contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;

d. include—

i. a description of the—

(aa) nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and

(bb) type of communication which is required to be intercepted; and

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

e. if applicable, indicate 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 too dangerous to apply in order to obtain the required evidence: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in subsection (5)(a)(i) if the serious offence has been or is being or will probably be committed for the benefit of, at the direction of, or in association with, a criminal organisation;

f. indicate the period for which the interception direction is required to be issued;

g. indicate whether any previous application has been made for the issuing of an interception direction in respect of the same person or customer, facility or place specified in the application and, if such previous application exists, must indicate the current status of that application; and

h. comply with any supplementary directives relating to applications for interception directions issued under section 58.

(3) An application on a ground referred to in—

a. subsection (5)(a)(i), must be made by an applicant referred to in paragraph (a), **[or]** (d) or (f) of the definition of "applicant";

b. subsection (5)(a)(ii) or (iii), must be made by an applicant referred to in paragraph (b) or (c) of the definition of "applicant";

c. subsection (5)(a)(iv), must, in the case of—

i. the investigation of a serious offence, be made by an applicant referred to in paragraph (a) or (d) of the definition of "applicant"; and

ii. the gathering of information, be made by an applicant referred to in paragraph **[(b) or]** (c) of the definition of "applicant"; and

d. subsection (5)(a)(v), must be made by an applicant referred to in paragraph (e) of the definition of "applicant":

Provided that an applicant referred to in paragraph (f) of the definition of "applicant" may only make an application on the ground referred to in subsection (5)(a)(i)—

i. if the offence allegedly has been or is being or will be committed by a member of the Police Service; or

ii. in respect of a death in police custody or as a result of police action.

(4) Notwithstanding section 2 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of subsection (1), issue an interception direction.

(5) An interception direction may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned that—

a. there are reasonable grounds to believe that—

i. a serious offence has been or is being or will probably be committed;

ii. the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

iii. the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

iv. the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to

organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

(aa) accordance with an international mutual assistance agreement; or
(bb) the interests of the Republic's international relations or obligations; or

v. the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;

b. there are reasonable grounds to believe that the—

i. interception of particular communications concerning the relevant ground referred to in paragraph (a) will be obtained by means of such an interception direction; and

ii. facilities from which, or the place where, the communications to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (a) are commonly used by the person or customer in respect of whom the application for the issuing of an interception direction is made; and

c. in respect of the grounds referred to in paragraph (a)(i), (iii), (iv) or (v), other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner.

(6) An interception direction—

a. must be in writing;

b. must contain the information referred to in subsection (2)(a)(ii) and (iii) and (d)(i);

c. may specify conditions or restrictions relating to the interception of communications authorised therein; and

d. may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein.

(7) (a) An application must be considered and an interception direction issued without any notice to the person or customer to whom the application applies and without hearing such person or customer.

b. A designated judge considering an application may require the applicant to furnish such further information as he or she deems necessary.

Application for, and issuing of, [supplementary direction or] real-time communication-related direction

17. (1) If**[—**

a. an interception direction has been issued, the applicant who made the application in respect of the interception direction concerned or, if he or she is not available, any other applicant who would have been entitled to make that application; or

b. **]** no interception direction has been issued**[, an applicant, if in a specific case]** and only real-time communication-related information on an ongoing basis **[without the actual interception of an indirect communication]** is required,

an applicant may apply to a designated judge**[, in the case of—**

i. paragraph (a), for the issuing of a supplementary direction; or

ii. **paragraph (b),]** for the issuing of a real-time communication-related direction.

(2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must—

a. [contain, with the necessary changes, the information referred to in section 15(2)(a), (c), (d), (e), (f) and (g);

b. in the case of subsection (1)(a)—

i. contain an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;

ii. contain proof that an interception direction has been issued; and

iii. be made at any stage after the issuing of the interception direction concerned, but before the expiry of the period or extended period for which it has been issued;

c. in the case of subsection (1)(b), also contain, with the necessary changes, the information referred to in section 15(2)(b); and

d. **comply with any supplementary directives relating to applications for supplementary directions or] real-time communication-related directions issued under section 55.]**

a. indicate the identity of the—

i. applicant;

ii. customer, if known, in respect of whom the real-time communication-related information is required; and

iii. telecommunication service provider to whom the real-time communication-related direction must be addressed;

b. specify the ground referred to in subsection (4) on which the application is made;

c. contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;

d. include—

i. a description of the type of real-time communication-related information that is required; and

ii. the basis for believing that evidence relating to the ground on which the application is made will be obtained through the provision of the real-time communication-related information;

e. indicate whether the real-time communication-related information must be—

i. routed to a designated interception centre specified in the application; or

ii. provided to the Police Service, the Defence Force, the Agency, the Service, the Directorate or the National Director, as the case may be;

f. indicate the period for which, and the manner in which, the archived communication-related information is required to be provided;

g. indicate whether any previous application has been made for the issuing of a real-time communication-related direction in respect of the same customer or real-time communication-related information specified in the application and, if such previous application exists, must indicate the current status of that application; and

h. comply with any supplementary directives relating to applications for real-time communication-related directions issued under section 58.

[(3) Section 14(3) applies, with the necessary changes, in respect of an application for the issuing of a real-time communication-related direction.]

(3) Notwithstanding section 12 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of subsection (1), issue **[a supplementary direction or]** a real-time communication-related direction**[, as the case may be]**.

(4) A **[supplementary direction or a]** real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds 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 public health or safety, national security or compelling national economic interests of the Republic is necessary;

c. the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

d. the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

i. accordance with an international mutual assistance agreement; or

ii. the interests of the Republic's international relations or obligations; or

e. the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

f. and that the provision of **[archived]** real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.

(5) A **[supplementary direction or a]** real-time communication-related direction—

a. must be in writing;

b. must contain the information referred to in subsection **[15]**(2)(a)(ii) and (iii), (d)(i) and (e);

c. may specify conditions or restrictions relating to the provision of real-time communication-related information authorised therein; and

d. may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein**[: Provided that a supplementary direction expires when the period or extended period for which the interception direction concerned has been issued, lapses]**.

(6) Section 16(3) and (7) applies, with the necessary changes, in respect of an application for, and the issuing of, **[a supplementary direction and]** a real-time communication-related direction.

Combined application for, and issuing of, interception direction, archived communication-related direction and real-time communication-related direction or interception direction supplemented by real-time communication-related direction

18. (1) If**[, in a specific case,]** the—

a. interception of an indirect communication and the provision of communication-related information, whether archived or real-time or both; or

b. provision of archived and real-time communication-related information,

are required, an applicant may, subject to sections 16(2) and (3), 17(1) and (2) **[and (3)]** and 19(1) and (2), in a combined application, apply to a designated judge for the simultaneous issuing of any combination of directions referred to in those sections.

(2) (a) If an interception direction has been issued in terms of section 16, the applicant who made the application in respect of the interception direction concerned or, if he or she is not available, any other applicant who would have been entitled to make that application, may, subject to section 17(1) and (2), apply to a designated judge for the issuing of a real-time communication-related direction to supplement that interception direction.

b. An application referred to in paragraph (a) must—

i. contain an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;

ii. contain proof that an interception direction has been issued; and

iii. be made at any stage after the issuing of the interception direction concerned, but before the expiry of the period or extended period for which it has been issued.

(3) A designated judge may, upon an application made to him or her in terms of—

a. subsection (1)(a) and subject to sections 16(4), (5), (6) and (7), 17**[(4), (5), (6) and (7)]** (3), (4), (5) and (6) and 19(3), (4), (5) and (6), issue the combination of directions applied for; or

b. subsection (1)(b) and subject to section 17 (3), (4), (5) and (6), issue a real-time communication-related direction to supplement that interception direction: Provided that a real-time communication-related direction issued under this paragraph expires when the period or extended period for which the interception direction concerned has been issued, lapses.

(4) Notwithstanding section 19(1), (3) and (4)—

a. an application in terms of subsection (1) for the issuing of an archived communication-related direction may only be made to a designated judge; and

b. only a designated judge may issue an archived communication-related direction in terms of subsection **[(2)]**(3).

Application for, and issuing of, archived communication-related direction

19. (1) If**[, in a specific case,]** only archived communication-related information **[without the actual interception of an indirect communication]** is required, an applicant may apply to a judge of a High Court, a regional court magistrate or a magistrate for the issuing of an archived communication-related direction.

(2) An application referred to in subsection (1) must be in writing and must—

a. [indicate the identity of the—

i. applicant;

ii. customer, if known, in respect of whom the archived communication-related information is required; and

iii. telecommunication service provider to whom the archived communication-related direction must be addressed;

b. specify the ground referred to in subsection (4) on which the application is made;

c. contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;

d. include—

i. a description of the type of archived communication-related information that is required; and

ii. the basis for believing that evidence relating to the ground on which the application is made will be obtained through the provision of the archived communication-related information;

e. indicate whether the archived communication-related information must be—

i. routed to a designated interception centre specified in the application; or

ii. provided to the Police Service, the Defence Force, the Agency, the Service, the Directorate or the National Director, as the case may be;

f. indicate the period for which, and the manner in which, the archived communication-related information is required to be provided;

g. indicate whether any previous application has been made for the issuing of an archived communication-related direction in respect of the same customer or archived communication-related information specified in the application and, if such previous application exists, must indicate the current status of that application;]

(a) contain, with the necessary changes, the information referred to in section 17(2); and

[(h)](b) comply with any supplementary directives relating to applications for archived communication-related directions issued under section 58.

(3) Notwithstanding section 12 or anything to the contrary in any other law contained, a judge of a High Court, a regional court magistrate or a magistrate may, upon an application made to him or her in terms of subsection (1), issue an archived communication-related direction.

(4) An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that there are reasonable grounds 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 public health or safety, national security or compelling national economic interests of the Republic is necessary;

c. the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

d. the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

i. accordance with an international mutual assistance agreement; or

ii. the interests of the Republic's international relations or obligations; or

e. the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.

(5) An archived communication-related direction—

a. must be in writing;

b. must contain the information referred to in **[subsection]** section 17(2)(a)(ii) and (iii), (d)(i) and (e);

c. must state the period within which the archived communication-related information must be provided; and

d. may specify conditions or restrictions relating to the provision of archived communication-related information authorised therein.

(6) Section 16(3) and (7) applies, with the necessary changes, in respect of an application for, and the issuing of, an archived communication-related direction.

(7) If a judge of a High Court, regional magistrate or magistrate issues an archive communication-related direction, he or she must, as soon as practicable thereafter, submit a copy of the application and archived communication-related direction concerned to a designated judge.

(8) A designated judge must keep **[a record of]** all copies of applications and archived communication-related directions submitted to him or her in terms of subsection (7).

Amendment or extension of existing direction

20. (1) The applicant who made the application in respect of an existing direction or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the existing direction concerned, but before the expiry of the period for which it has been issued, apply to a designated judge for an amendment thereof or the extension of the period for which it has been issued.

(2) An application referred to in subsection (1) must be in writing and must—

a. contain full particulars of the reasons and circumstances alleged by the applicant in support of his or her application;

b. in the case of an application for the—

i. amendment of an existing direction, indicate the amendment which is required; or

ii. extension of the period for which an existing direction has been issued, indicate the period for which the extension is required;

c. contain an affidavit setting forth the results obtained from the direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results; and

d. comply with any supplementary directives relating to applications for the amendment or extension of directions issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1)—

a. amend an existing direction; or

b. extend the period for which an existing direction has been issued.

(4) An existing direction may only be amended or the period for which it has been issued may only be extended if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that the amendment or extension is necessary for purposes of achieving the objectives of the direction concerned: Provided that the period for which an existing direction has been issued may only be extended for a further period not exceeding three months at a time.

(5) Any amendment of an existing direction or extension of the period for which it has been issued, must be in writing.

(6) Sections 16(7) and 24 apply, with the necessary changes, in respect of the amendment of an existing direction or the extension of the period for which an existing direction has been issued.

Application for, and issuing of, decryption direction

21. (1) An applicant who—

a. makes an application referred to in section 16(1) may in his or her application also apply for the issuing of a decryption direction; or

b. made an application referred to in section 16(1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of a decryption direction.

(2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must—

a. indicate the identity of the—

i. applicant;

ii. customer, if known, in respect of whom the decryption of encrypted information is required; and

iii. decryption key holder to whom the decryption direction must be addressed;

b. describe the encrypted information which is required to be decrypted;

c. specify the—

i. decryption key, if known, which must be disclosed; or

ii. decryption assistance which must be provided, and the form and manner in which it must be provided;

d. indicate the period for which the decryption direction is required to be issued;

e. indicate whether any previous application has been made for the issuing of a decryption direction in respect of the same customer or encrypted information specified in the application and, if such previous application exists, must indicate the current status of that application;

f. contain an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;

g. contain proof that an interception direction has been issued; and

h. comply with any supplementary directives relating to applications for decryption directions issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1), issue a decryption direction.

(4) A decryption direction may only be issued—

a. if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that there are reasonable grounds to believe that—

i. any indirect communication to which the interception direction concerned applies, or any part of such an indirect communication, consists of encrypted information;

ii. the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto;

iii. the purpose for which the interception direction concerned was issued would be defeated, in whole or in part, if the decryption direction was not issued; and

iv. it is not reasonably practicable for the authorised person who executes the interception direction concerned or assists with the execution thereof, to obtain possession of the encrypted information in an intelligible form without the issuing of a decryption direction; and

b. after the designated judge concerned has considered—

i. the extent and nature of any other encrypted information, in addition to the encrypted information in respect of which the decryption direction is to be issued, to which the decryption key concerned is also a decryption key; and

ii. any adverse effect that the issuing of the decryption direction might have on the business carried on by the decryption key holder to whom the decryption direction is addressed.

(5) A decryption direction—

a. must be in writing;

b. must contain the information referred to in subsection (2)(a)(ii) and (iii), (b) and (c);

c. must state the period within which the decryption key must be disclosed or the decryption assistance must be provided, whichever is applicable;

d. may specify conditions or restrictions relating to decryption authorised therein; and

e. may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein: Provided that a decryption direction expires when the period or extended period for which the interception direction concerned has been issued, lapses.

(6) Section 16(7) applies, with the necessary changes, in respect of the issuing of a decryption direction.

Application for, and issuing of, entry warrant

22. (1) An applicant who—

a. makes an application referred to in section 16(1) may in his or her application also apply for the issuing of an entry warrant; or

b. made an application referred to in section 16(1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of an entry warrant.

(2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must—

a. indicate—

i. the premises in respect of which the entry warrant is required to be issued; and

ii. the specific purpose, referred to in the definition of "entry warrant", for which the application is made;

b. if the application is made in terms of subsection (1)(b), also—

i. indicate the identity of the applicant;

ii. contain proof that an interception direction has been issued; and

iii. contain an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;

c. indicate whether any previous application has been made for the issuing of an entry warrant for the same purpose or in respect of the same premises specified in the application and, if such previous application exists, must indicate the current status of that application; and

d. comply with any supplementary directives relating to applications for entry warrants issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1), issue an entry warrant.

(4) An entry warrant may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that—

a. the entry of the premises concerned is necessary for a purpose referred to in the definition of "entry warrant"; or

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

(5) An entry warrant—

a. must be in writing;

b. must contain the information referred to in subsection (2)(a); and

c. may contain conditions or restrictions relating to the entry upon the premises concerned as the designated judge deems necessary.

(6) An entry warrant expires when—

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

b. it is cancelled in terms of section 25(1) or (3) by the designated judge who issued it or, if he or she is not available, by any other designated judge,

whichever occurs first.

(7) Section 16(7) applies, with the necessary changes, in respect of the issuing of an entry warrant.

(8) If an entry warrant has expired as contemplated in subsection (6)(a), the applicant who made the application in respect of the entry warrant concerned or, if he or she is not available, any other applicant who would have been entitled to make that application, must, as soon as practicable after the date of expiry of the entry warrant concerned, remove, or cause to be removed, any interception device which has been installed thereunder and which, at the date of expiry of that entry warrant, has not yet been removed from the premises concerned.

Oral application for, and issuing of, direction, entry warrant, oral direction or oral entry warrant

23. (1) Notwithstanding sections 16(2), 17(2), 21(2) and 22(2), an application referred to in section 16(1), 17(1), 18(1), 21(1) or 22(1) may be made orally if the applicant is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) Section 16(3), 17(1)(a) or (3), 21(1) or 22(1), whichever is applicable, applies, with the necessary changes, in respect of an oral application referred to in subsection (1).

(3) An oral application referred to in subsection (1) must—

a. contain the information referred to in section 16(2), 17(2), 21(2) or 22(2), whichever is applicable;

b. indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the applicant, justify the making of an oral application; and

c. comply with any supplementary directives relating to oral applications issued under section 58.

(4) Notwithstanding sections 2 and 12 or anything to the contrary in any other law contained, a designated judge may, upon an oral application made to him or her in terms of subsection (1), issue the direction or entry warrant applied for.

(5) A direction or an entry warrant may only be issued in terms of subsection (4)—

a. if the designated judge concerned is satisfied, on the facts alleged in the oral application concerned, that—

i. there are reasonable grounds to believe that the direction or entry warrant applied for could be issued;

ii. a direction is immediately necessary on a ground referred to in section 16(5)(a), 17(5) or 21(4)(a), whichever is applicable, or an entry warrant is immediately necessary for a purpose referred to in the definition of "entry warrant"; and

iii. it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of the direction or entry warrant applied for; and

b. on condition that the applicant concerned must submit a written application to the designated judge concerned within 48 hours after the issuing of the direction or entry warrant in terms of subsection (4).

(6) Section 16(5)(b) and (c), (6) and (7), 17(6) and (7), 21(4)(b), (5) and (6) or 22(5), (6), (7) and (8), whichever is applicable, applies, with the necessary changes, in respect of the issuing of a direction or an entry warrant in terms of subsection (4).

(7) Notwithstanding—

a. sections 2 and 12 or anything to the contrary in any other law contained; and

b. section 16(6)(a), 17(6)(a), 21(5)(a) or 22(5)(a), whichever is applicable,

c. a designated judge may, upon an oral application made to him or her in terms of subsection (1), orally issue the direction or entry warrant applied for.

(8) An oral direction or oral entry warrant may only be issued in terms of subsection (7)—

a. if the designated judge concerned is satisfied, on the facts alleged in the oral application concerned, that—

i. there are reasonable grounds to believe that the direction or entry warrant applied for could be issued;

ii. a direction is immediately necessary on a ground referred to in section 16(5)(a), 17(5) or 21(4)(a), whichever is applicable, or an entry warrant is immediately necessary for a purpose referred to in the definition of "entry warrant"; and

iii. it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for, and to issue in writing, the direction or entry warrant applied for; or

iv. any other exceptional circumstances exist which justify the issuing of an oral direction or oral entry warrant; and

b. on condition that the applicant concerned must submit a written application to the designated judge concerned within 48 hours after the issuing of the oral direction or oral entry warrant in terms of subsection (7).

(9) Section 16(5)(b) and (c), (6)(b), (c) and (d) and (7), 17(6)(b), (c) and (d) and (7), 21(4)(b), (5)(b), (c), (d) and (e) and (6) or 22(5)(b) and (c), (6), (7) and (8), applies, with the necessary changes, in respect of the issuing of an oral direction or oral entry warrant.

(10) A designated judge who issues an oral direction or oral entry warrant in terms of subsection (7)—

a. or any person authorised thereto in writing by him or her, must, as soon as practicable thereafter, inform the applicant and, if applicable, the postal service provider or telecommunication service provider to whom it is addressed, in writing of such an oral direction or oral entry warrant, including—

i. the contents thereof; and

ii. the period for which it has been issued; and

b. must, subject to section 25, confirm that oral direction or oral entry warrant in writing within 24 hours after the receipt of the written application referred to in subsection (8)(b).

Reports on progress

24. The designated judge who issued a direction or an entry warrant may at the issuing thereof or at any stage **[after the issuing thereof, but]** before the date of expiry thereof, **[in the case of—**

a. (a) a direction, of the period or extended period for which it has been issued; or

b. (b) an entry warrant, of the period or extended period for which the interception direction concerned has been issued,]

in writing require the applicant who made the application in respect of the direction or entry warrant concerned to report to him or her in writing—

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

i. the progress that has been made towards achieving the objectives of the direction or entry warrant concerned; and

ii. any other matter which the designated judge deems necessary; or

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

Cancellation of direction, entry warrant, oral direction or oral entry warrant

25. (1) The designated judge who issued a direction or an entry warrant or, if he or she is not available, any other designated judge who would have been entitled to issue such direction or entry warrant may cancel that direction or entry warrant if—

a. the applicant concerned fails to submit a report in terms of section 24**[(1)]**, if applicable; or

b. he or she, upon receipt of a report submitted in terms of section 24**[(1)]**, is satisfied that the—

i. objectives of the direction or entry warrant concerned have been achieved; or

ii. ground on which the direction or the purpose for which the entry warrant concerned was issued, has ceased to exist.

(2) The designated judge who issued—

a. a direction or an entry warrant in terms of section 23(4); or

b. an oral direction or oral entry warrant in terms of section 23(7),

c. or, if he or she is not available, any other designated judge who would have been entitled to issue such a direction, entry warrant, oral direction or oral entry warrant, must cancel that direction, entry warrant, oral direction or oral entry warrant if—

i. the applicant concerned fails to comply with section 23(5)(b) or (8)(b); or

ii. he or she, upon receipt of a written application contemplated in section 23(5)(b) or (8)(b), is satisfied, on the facts alleged in that application, that the direction, entry warrant, oral direction or oral entry warrant concerned should not have been issued.

(3) If a designated judge cancels—

a. a direction or an entry warrant;

b. a direction or entry warrant issued under section 23(4); or

c. an oral direction or oral entry warrant,

in terms of subsection (1) or (2) he or she must forthwith in writing inform—

i. the applicant concerned; and

ii. if applicable, the postal service provider, telecommunication service provider or decryption key holder concerned,

of such cancellation.

(4) If an entry warrant or oral entry warrant is cancelled in terms of subsection (1) or (2), the applicant concerned must, as soon as practicable after having been informed of such cancellation, remove, or cause to be removed, any interception device which has been installed under the entry warrant or oral entry warrant concerned.

(5) If a direction issued under section 23(4) or an oral direction is cancelled in terms of subsection (2)—

a. the contents of any communication intercepted under that direction or oral direction will be inadmissible as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, unless the court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice; or

b. any postal article that was taken into possession under that direction or oral direction must be dealt with in accordance with section 26(4).

CHAPTER 4

EXECUTION OF DIRECTIONS AND ENTRY WARRANTS

Execution of direction

26. (1) (a) If a direction has been issued under this Act, any—

[(a)](i) law enforcement officer may execute that direction; or

[(b)](ii) law enforcement officer or other person may assist with the execution thereof,

if the law enforcement officer or person concerned has been authorised by the applicant who made the application for the issuing of the direction concerned to execute that direction or to assist with the execution thereof.

b. A direction issued under this Act upon an application made by an applicant referred to in paragraph (f) of the definition of "applicant" may only be executed by a law enforcement officer authorised thereto in writing by the applicant concerned, after consultation with the Police Service, Defence Force, Agency or Service, as the case may be, of which that law enforcement officer is a member, or the National Director if that law enforcement officer is a member of the prosecuting authority.

(2) The applicant concerned may authorise such number of authorised persons to assist with the execution of the direction as he or she deems necessary.

(3) An authorised person who executes a direction or assists with the execution thereof may intercept, at any place in the Republic, any communication in the course of its occurrence or transmission to which the direction applies.

(4) If any postal article has been taken in possession in terms of subsection (3), the authorised person who executes the direction concerned or assists with the execution thereof—

a. must take proper care of such postal article and may, if the postal article concerned is perishable, with due regard to the interests of the persons concerned and with the written approval of the applicant concerned, dispose of that postal article in such manner as the circumstances may require;

b. must, with the written approval of the applicant concerned, return such postal article, if it has not been disposed of in terms of paragraph (a), or cause it to be returned to the postal service provider concerned if, in the opinion of the applicant concerned—

i. no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, will be instituted in connection with such postal article; or

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

iii. such postal article may be returned without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be; or

c. may, in circumstances other than those referred to in —

i. paragraph (b), with the written approval of the applicant concerned, return such postal article or cause it to be returned to the postal service provider concerned if such postal article—

(aa) has not been disposed of in terms of paragraph (a); and

(bb) in the opinion of the applicant concerned, may be returned without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be; or

ii. paragraph (a), on the written instructions of the applicant concerned dispose of such postal article in such manner as the public health or safety, national security or compelling national economic interests of the Republic, as the case may be, requires, if such postal article—

(aa) has not been disposed of in terms of paragraph (a); and

(bb) in the opinion of the applicant concerned, cannot be returned in terms of subparagraph (i) without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be.

Execution of entry warrant

27. **[(1)]** If an entry warrant has been issued, any authorised person who executes the interception direction in respect of which that entry warrant has been issued or assists with the execution thereof may, at any time during which the entry warrant is of force, without prior notice enter the premises specified in the entry warrant and perform any act relating to the purpose, referred to in the definition of "entry warrant", for which the entry warrant concerned has been issued.

[(2) If, during the execution of an entry warrant, a person claims that any postal article found on or in the premises contains privileged information and refuses the inspection or removal of such postal article, the authorised person who executes the entry warrant may request a judge to cause that postal article to be seized and removed for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not.]

Assistance by postal service provider and telecommunication service provider

28. (1) If an interception direction or a copy thereof is handed to the postal service provider or telecommunication service provider to whom the interception direction is addressed by the authorised person who executes that interception direction or assists with the execution thereof, the—

a. postal service provider concerned must intercept the postal article to which the interception direction applies and hand it to the authorised person concerned; or

b. telecommunication service provider concerned must **[as soon as practicable]** immediately—

(i) route the duplicate signals of indirect communications to which that interception direction applies to the designated interception centre concerned; or

[(i)](ii) make available the necessary assistance and, subject to section 46(7)(b), the necessary facilities and devices to enable the authorised person concerned, to effect the necessary connections in order to intercept any indirect communications to which the interception direction applies**[; or**

(ii) route the duplicate signals of indirect communications to which that interception direction applies to the designated interception centre concerned].

(2) If an archived communication-related direction or a real-time communication-related direction **[or a supplementary direction]** or a copy thereof is handed to the telecommunication service provider to whom the archived communication-related direction or real-time communication-related direction **[or supplementary direction]** is addressed by the authorised person who executes that archived communication-related direction or real-time communication-related direction **[or supplementary direction]** or assists with the execution thereof, the telecommunication service provider concerned must—

a. route the—

(i) archived communication-related information specified in the archived communication-related direction concerned; or

(ii) real-time communication-related information specified in the real-time communication-related direction **[or supplementary direction]** concerned as soon as practicable after it became available,

to the designated interception centre concerned; or

b. provide the—

i. archived communication-related information specified, and within the period stated, in the archived communication-related direction concerned; or

ii. real-time communication-related information specified in the real-time communication-related direction **[or supplementary direction]** concerned as soon as practicable after it became available,

to the Police Service, the Defence Force, the Agency, the Service, the Directorate or the National Director, as the case may be, in the form as specified in that archived communication-related direction or real-time communication-related direction **[or supplementary direction]**.

Assistance by decryption key holder

29. (1) If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the authorised person who executes that decryption direction or assists with the execution thereof, the decryption key holder concerned must within the period stated in the decryption direction—

a. disclose the decryption key; or

b. provide the decryption assistance,

specified in the decryption direction concerned, to the authorised person concerned**[: Provided that a telecommunication service provider is only responsible for decrypting any indirect communication encrypted by a customer if the facility for encryption was provided by the telecommunication service provider concerned]**.

(2) In complying with a decryption direction, a decryption key holder—

a. must only disclose such decryption key or provide such decryption assistance which is necessary to obtain access to the encrypted information specified in that decryption direction or to put that encrypted information in an intelligible form;

b. may only disclose the decryption key or provide the decryption assistance to the authorised person who executes that decryption direction or assists with the execution thereof; and

c. may not disclose any other information, which is not specified in that decryption direction, relating to the customer in respect of whose encrypted information the decryption key has been disclosed or the decryption assistance has been provided.

(3) A decryption key holder to whom a decryption direction is addressed and who is in possession of both the encrypted information and the decryption key thereto—

a. may use any decryption key in his or her possession to provide decryption assistance; and

b. must, in providing such decryption assistance, make a disclosure of the encrypted information in an intelligible form.

(4) A decryption key holder who, in terms of a decryption direction, is required to provide decryption assistance in respect of any encrypted information, will be regarded as having complied with that requirement if he or she—

a. in stead of providing such decryption assistance, discloses any decryption key to the encrypted information that is in his or her possession; and

b. makes such a disclosure, in accordance with the decryption direction concerned, to the authorised person to whom, and by the time by which, he or she was required to provide the decryption assistance.

(5) If a decryption key holder to whom a decryption direction is addressed, is—

a. not in possession of the encrypted information; or

b. incapable, without the use of a decryption key that is not in his or her possession, to provide decryption assistance,

the decryption key holder concerned will, in accordance with the decryption direction concerned, be required**[—**

i. **]** to comply, to the best of his or her ability, with that decryption direction**[; or**

ii. **to assist, to the best of his or her ability, any other decryption key holder to whom a decryption direction in respect of the same encrypted information has been addressed, in disclosing the decryption key or providing the decryption assistance specified in that decryption direction]**.

(6) If a decryption key holder to whom a decryption direction is addressed, is in possession of different decryption keys, or combinations of decryption keys, to the encrypted information—

a. it will not be necessary, for purposes of complying with the decryption direction concerned, for the decryption key holder to disclose any decryption 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 encrypted information and to put it into an intelligible form; or

b. the decryption key holder may select which of the decryption keys, or combination of decryption keys, to disclose for purposes of complying with the decryption direction concerned.

(7) If a decryption direction is addressed to a decryption key holder who—

a. has been in possession of the decryption key to the encrypted information, but is no longer in possession thereof;

b. if he or she had continued to have the decryption key in his or her possession, he or she would have been required by virtue of the decryption direction to disclose it; and

c. is in possession of any information that would facilitate the obtaining or discovery of the decryption key or the provision of decryption assistance,

he or she will be required, in accordance with the decryption direction, to disclose all such information as is in his or her possession to the authorised person who executes the decryption direction or assists with the execution thereof.

(8) An authorised person to whom a decryption key has been disclosed under this section—

a. may use the decryption key only in respect of the encrypted information, and in the manner and for the purposes, specified in the decryption direction concerned; and

b. must, on or before the expiry of the period or extended period for which the decryption direction concerned has been issued, with the written approval of the applicant who made the application for the issuing of a decryption direction, destroy all records of the disclosed decryption key if, in the opinion of the applicant concerned—

i. no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 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 an order of court.

CHAPTER 5

INTERCEPTION CAPABILITY AND [REMUNERATION] <u>COMPENSATION</u>

Interception capability of telecommunication services and storing of communication-related information

30. (1) Notwithstanding any other law, a telecommunication service provider must—

a. provide a telecommunication service which has the capability to be intercepted; and

b. store communication-related information.

(2) The Minister of Communications, in consultation with the Minister and the other relevant Ministers and after consultation with <u>the Authority and</u> a telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Telecommunications Act, to such a telecommunication service provider or category of telecommunication service providers—

a. issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the—

i. manner in which effect is to be given to subsection (1) by the telecommunication service provider or category of telecommunication service providers concerned;

ii. facilities and devices to be acquired by the telecommunication service provider or category of telecommunication service providers to enable the—

(aa) interception of indirect communications in terms of this Act; and
(bb) storing of communication-related information in terms of subsection (1)(b); and

iii. type of communication-related information which must be stored in terms of subsection (1)(b) and the period for which such information must be stored, which period may not be less than **[2]** three years from the date of the transmission of the indirect communication to which that communication-related information relates; and

b. determine a period, which may not be less than three months and not more than **[6]** six months from the date on which a directive referred to in paragraph *(a)* is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

(3) A directive referred to in subsection (2)*(a)*—

a. must, if applicable, prescribe—

i. the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2)(a)(ii);

ii. the capacity needed for interception purposes;

iii. the systems to be used;

iv. the connectivity with interception centres referred to in section 32;

v. the manner of routing duplicate signals of indirect communications to designated interception centres in terms of section 28(1)(b)(ii);

vi. the manner of routing archived or real-time communication-related information to designated interception centres in terms of section 28(2)(a); and

b. may prescribe any other matter which the Minister of Communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority, deems necessary or expedient.

(4) Notwithstanding any other law, agreement or licence, a telecommunication service provider must, subject to section 46(1), at own cost acquire, whether by purchasing or leasing, the facilities and devices determined in a directive referred to in subsection (2)(a).

(5) Any costs incurred by a telecommunication service provider in enabling—

a. a telecommunication service to be intercepted; and

b. communication-related information to be stored,

including the investment, technical, maintenance and operating costs, must be carried by the telecommunication service provider providing such a service and storing such information.

(6) A directive issued under subsection (2)(a) may in like manner be amended or withdrawn.

(7) The Minister of Communications must, within two months after the fixed date and in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and a telecommunication service provider or category of telecommunication service providers to whom, prior to the fixed date, a telecommunication service licence has been issued under the Telecommunications Act**[, prior to the fixed date]**—

a. issue a directive referred to in subsection (2)(a) in respect of such a telecommunication service provider or category of telecommunication service providers; and

b. determine a period, which may not be less than three months and not more than **[6]** six months from the date on which a directive referred to in paragraph *(a)* is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

[Remuneration] Compensation payable to postal service provider, telecommunication service provider and decryption key holder

31. (1) (a) The Minister, after consultation with the Ministers of Communications and Finance and the postal service providers or telecommunication service providers concerned, as the case may be, must by notice in the *Gazette* prescribe—

i. the forms of assistance in the execution of a direction for which a postal service provider, telecommunication service provider or decryption key holder must be **[remunerated]** compensated; and

ii. reasonable tariffs of **[remuneration]** compensation payable to a postal service provider, telecommunication service provider or decryption key holder for providing such prescribed forms of assistance.

b. The tariffs prescribed under paragraph (a)(ii)—

i. may differ in respect of different categories of postal service providers, telecommunication service providers or decryption key holders; and

ii. must be uniform in respect of each postal service provider, telecommunication service provider or decryption key holder falling within the same category.

c. A notice issued under paragraph (a) may at any time in like manner be amended or withdrawn.

d. The first notice to be issued under paragraph (a) must be published in the *Gazette* within three months after the fixed date.

(2) The forms of assistance referred to in subsection (1)(a)(i) must include, in the case of—

a. a telecommunication service provider, the—

i. making available of a facility, device or telecommunications system;

ii. provision or routing of archived or real-time communication-related information; and

iii. routing of duplicate signals of indirect communications; and

b. a decryption key holder, the—

i. disclosure of a decryption key; and

ii. provision of decryption assistance.

(3) The **[remuneration]** compensation payable to a postal service provider, telecommunication service provider or decryption key holder in terms of this section will only be**[—**

a. **]** for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance contemplated in subsection (1)(a)(i)**[; and**

b. **in the case of a telecommunication service provider, for the lease of telecommunication facilities, where applicable, by the telecommunication service provider concerned to the Police Service, Defence Force, Agency, Service, Directorate or prosecuting authority]**.

(4) Any notice issued under subsection (1) must, before publication thereof in the *Gazette*, be submitted to Parliament.

CHAPTER 6

INTERCEPTION CENTRES, OFFICE FOR INTERCEPTION CENTRES AND [INTERCEPTION] INTERNET SERVICE PROVIDERS ASSISTANCE FUND

Establishment of interception centres

32. (1) The Minister, in consultation with the relevant Ministers, must, at State expense establish one or more centres to be known as interception centres for the interception of communications in terms of this Act.

(2) The Minister of Communications, in consultation with the Minister and the other relevant Ministers and after consultation with a telecommunication service provider or category of telecommunication service providers must, within two months after the date contemplated in section 30(2)(b) or (7)(b)—

a. issue a directive in respect of the Police Service, the Defence Force, the Agency, the Service, the Directorate and the National Director, determining the—

i. manner in which effect is to be given to subsection (1)(b); and

ii. connections to be acquired to enable the routing of—

(aa) duplicate signals of indirect communications; and
(bb) archived and real-time communication-related information,

to interception centres in terms of this Act; and

b. determine a period, which may not be less than three months and not more than 12 months from the date on which a directive referred to in paragraph *(a)* is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

(3) A directive referred to in subsection (2)*(a)*—

a. must prescribe—

i. the security, technical and functional requirements of the connections to be acquired in terms of subsection (2)(a)(ii) to ensure compatibility between telecommunication systems and interception centres which are connected by the connections concerned; and

ii. the connectivity with telecommunication systems;

a. may prescribe any other matter which the Minister of Communications, in consultation with the Minister and the other relevant Ministers and after consultation with the telecommunication service provider or category of telecommunication service providers concerned, deems necessary or expedient to ensure.

(4) A directive issued under subsection (2)(a) may in like manner be amended or withdrawn.

(5) An interception centre will, for purposes of performing its functions in terms of this Act, be exempted from—

a. obtaining any kind of licence required by the Telecommunications Act; and

b. paying any fees payable in terms of that Act.

(6) The Minister and the relevant Ministers will jointly be responsible for any expenditure incidental to the—

a. establishing, equipping, operating and maintaining of interception centres;

b. acquiring, installing and maintaining of connections between telecommunication systems and interception centres; and

c. administration and functioning of interception centres.

(7) The Minister of Defence, in consultation with the Minister and the other relevant Ministers, may under section 2 of the National Key Points Act, 1980 (Act No. 102 of 1980), declare an interception centre a National Key Point.

Establishment of Office for Interception Centres

33. (1) There is hereby established an office to be known as the Office for Interception Centres.

(2) The Minister and the relevant Ministers will jointly be responsible for any expenditure incidental to the administration and functioning of the Office.

Director and staff of Office

34. (1) The Minister and the relevant Ministers must, from among their respective Departments, second a member or an officer to the office of Director: Office for Interception Centres, who will be the head of the Office.

(2) The Director may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, subject to the control and directions of the Minister.

(3) Whenever the Director is for any reason unable to exercise, perform and carry out his or her powers, functions and duties or when the secondment of a member or an officer as Director is pending, the Minister and the relevant Ministers may, from among their respective Departments, designate a member or an officer to the service of the Office as Acting Director, to exercise the powers, perform the functions and carry out the duties of the Director.

(4) The Minister and the relevant Ministers may, from among their respective Departments, second a member or an officer to the office of Deputy Director: Office for Interception Centres, who, subject to the control and directions of the Director, may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director.

(5) The Director will in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, be assisted, subject to his or her control and directions, by—

a. members of the Police Service, Defence Force, Agency, Service and prosecuting authority designated to the service of the Office for that purpose by the—

i. National Commissioner: South African Police Service;

ii. Secretary for Defence;

iii. Director-General: National Intelligence Agency;

iv. Director-General: South African Secret Service; and

v. National Director of Public Prosecutions; and

b. officers of any other Department of State seconded to the service of the Office, for a particular service.

(6) Any secondment and designation contemplated in this section and section 36—

a. must, where applicable, be done in terms of the laws regulating such secondment; and

b. may only be done with the consent of the member or officer concerned.

Powers, functions and duties of Director

35. (1) In order to achieve the objects of this Act, the Director—

a. must carry out the administrative duties relating to the functioning of the Office;

b. must exercise control over heads of interception centres and staff of the Office;

c. must manage, and exercise administrative control over, interception centres;

d. must regulate the procedure and determine the manner in which the provisions of this Act must be carried out by interception centres;

e. must co-ordinate the activities of interception centres;

f. must ensure that a head of an interception centre complies with directives issued under section 32(2)(a);

g. must prescribe the information to be kept by the head of an interception centre in terms of section 37, which must include particulars relating to—

i. applications for the issuing of directions and the directions issued upon such applications which is relevant to the interception centre of which he or she is the head; and

ii. the results obtained from every direction executed at that interception centre;

h. must prescribe the manner in, and the period for, which such information must be kept; and

i. is, for purposes of the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, be accountable to the Minister.

(2) A member or an officer designated or seconded in terms of section 34(5) may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director, subject to the control and directions of the Director.

(3) The Police Service, Defence Force, Agency, Service, prosecuting authority and other Departments of State must render such assistance as may be reasonably required in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon the Director by the Minister or under this Act.

Head and staff of interception centres

36. (1) The Minister must in respect of every interception centre to be established by section 32(1), request the persons referred to in section 34(5)(a)(i) to (v) to second a member from among their respective Departments to such interception centre as head of the interception centre in terms of the laws regulating such secondment.

(2) The head of an interception centre may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director or under this Act, subject to the control and directions of the Director.

(3) Whenever the head of an interception centre is for any reason unable to exercise, perform and carry out his or her powers, functions and duties or when the secondment of a member as head of an interception centre is pending, the Minister may request the persons referred to in section 34(5)(a)(i) to (v), to designate, from among their respective Departments, a member to the service of that interception centre as acting head of the interception centre concerned, to exercise the powers, perform the functions and carry out the duties of the head of that interception centre.

(4) The head of an interception centre will in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director or under this Act, be assisted, subject to his or her control and directions, by other members of the Police Service, Defence Force, Agency, Service and prosecuting authority, designated to the service of the interception centre concerned for that purpose by the persons referred to in section 34(5)(a)(i) to (v).

(5) A member designated in terms of subsection (4) may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director or the head of the interception centre concerned, subject to the control and directions of the head of the interception concerned.

(6) In order to achieve the objects of this Act, the head of an interception centre must—

a. at state expense and in accordance with any directives issued under section 32(2)(a)—

i. equip, operate and maintain the interception centre concerned; and

ii. acquire, install and maintain a connection between a telecommunication system and the interception centre concerned; and

b. exercise control over members designated to the service of the interception centre in terms of subsection (4).

Keeping of records by heads of interception centres and submission of reports to Director

37. (1) The head of an interception centre must keep or cause to be kept proper records of such information as may be prescribed by the Director in terms of section 35(1)(g).

(2) (a) The head of an interception centre must on a quarterly basis, or as often as the Director requires, submit a written report to the Director on—

i. the records kept by him or her in terms of subsection (1);

ii. any abuses in connection with the execution of directions of which he or she is aware of;

iii. any defects in any telecommunication system or in the operation of the interception centre which have been discovered; and

iv. such activities at the interception centre or on any other matter relating to this Act which the Director requests the head of the interception to deal with in such report.

b. Notwithstanding paragraph (a), a head of an interception centre may at any stage submit a report to the Director on any matter which, in the opinion of the head concerned, should urgently be brought to the attention of the Director.

(3) The Director must, upon receipt of a report contemplated in subsection (2)(a), submit a copy of that report to the Minister and the Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act No. 40 of 1994).

Establishment and control of [Interception] Internet Service Providers Assistance Fund

38. (1) There is hereby established a fund to be known as the **[Interception]** Internet Service Providers Assistance Fund.

(2) The Fund will be credited with—

a. the contributions referred to in section 46(1)(b);

b. interest derived from the investment of money in the Fund; and

c. money accruing to the Fund from any other source.

(3) The money in the Fund must be utilised for—

a. acquiring, whether by purchasing or leasing, facilities and devices for purposes of section 46(7)(b); and

b. the expenses involved in the control and management of the Fund.

(4) The Director is the accounting officer of the Fund in terms of the Public Finance Management Act, 1999 (Act No. 1 of 1999).

(5) The Fund is, subject to the directions of the Minister, under the control and management of the Director, who—

a. must utilize the money in the Fund in accordance with subsection (3);

b. will be charged with the responsibility of accounting for money received in, and payments made from, the Fund; and

c. must cause the necessary accounting and other related records to be kept.

(6) **[(a)]** The Minister of Intelligence, in consultation with the Minister and other relevant Ministers, must **[establish an Advisory Committee consisting of—**

i. a member of the Police Service, appointed by the National Commissioner: South African Police Service;

ii. a member of the Defence Force, appointed by the Secretary for Defence;

iii. a member of the Agency, appointed by the Director-General: National Intelligence Agency;

iv. a member of the Service, appointed by the Director-General: South African Secret Service;

v. a member of the prosecuting authority, appointed by the National Director of Public Prosecutions; and

vi. an officer in the Department of Communications, appointed by the Director-General: Department of Communications.

b. **The Advisory Committee must]** make recommendations to the Director relating to the utilisation of the money in the Fund as contemplated in subsection (3)(a)

(7) Any money in the Fund which is not required for immediate use must be invested by the Director with a banking institution approved by the Minister, in consultation with the Minister of Finance, and may be withdrawn when required.

(8) Any unexpended balance of the money in the Fund at the end of any financial year must be carried forward as a credit in the Fund to the next financial year.

(9) The Fund and the records referred to in subsection (5)(c) must be audited by the Auditor-General.

CHAPTER 7

DUTIES OF TELECOMMUNICATION SERVICE PROVIDER AND CUSTOMER

Information to be obtained and kept by certain telecommunication service provider

39. (1) Before a telecommunication service provider, other than a telecommunication service provider who provides a mobile cellular telecommunication service, enters into a contract with any person for the provision of a telecommunication service to that person, he or she—

a. must, if that person is a natural person—

(i) obtain from him or her—

(aa) his or her full names, identity number, residential and business or postal address, whichever is applicable; and
(bb) a certified photocopy **[of that page]** of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear **[and must]**;

(ii) retain **[such]** the photocopy obtained in terms of subparagraph (i)(bb); and

[(ii)](iii) verify the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; or

b. must, if that person is a juristic person—

i. obtain from the person representing that juristic person—

(aa) his or her full names, identity number, residential and postal address, whichever is applicable;

(bb) the business name and address and, if registered as such in terms of any law, the registration number of that juristic person;

(cc) a certified photocopy **[of that page]** of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear; and

(dd) a certified photocopy of the business letterhead of, or other similar document relating to, that juristic person;

ii. retain the photocopies obtained in terms of subparagraph (i)(cc) and (dd); and

iii. verify—

(aa) the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; and

(bb) the name and registration number of that juristic person with reference to its business letterhead or other similar document; and

c. may obtain from such person any other information which the telecommunication service provider deems necessary for purposes of this Act.

(2) A telecommunication service provider referred to in subsection (1) must ensure that proper records are kept of—

a. the information, including the photocopies, referred to in subsection (1) and, where applicable, any change in such information which is brought to his or her attention; and

b. any other information in respect of the person concerned which the telecommunication service provider concerned may require in order to enable him or her to identify that person, including the telephone number or any other number allocated to that person.

[(3) A telecommunication service provider referred to in subsection (1) must provide the Police Service, the Defence Force, the Agency, the Service, the Directorate or the National Director with such information regarding a customer, as may be required in writing by the relevant applicant or an authorised person who executes a direction or assists with the execution thereof, to perform the functions and exercise the powers authorised by law.

(4) The obligation in terms of subsection (3) includes the provision of the information and the furnishing of the photocopies referred to in subsection (1).]

(3) An applicant may, for purposes of making an application for the issuing of a direction, in writing request a telecommunication service provider referred to in subsection (1) to—

a. confirm that the person specified in the request is a customer of that telecommunication service provider concerned;

b. provide the applicant with the telephone number or any other number allocated to that person by that telecommunication service provider; and

c. furnish the applicant with a copy of the photocopy of the identification document of that person which is retained by that telecommunication service provider in terms of subsection (1)(a)(ii).

(4) A telecommunication service provider who receives a request referred to in subsection (3) must, as soon as practicable after such receipt, comply with that request if the person specified in the request is a customer of the telecommunication service provider concerned.

Information to be obtained and kept in respect of cellular phone and SIM-card

40. (1) Before any person sells, or in any other manner provides, any cellular phone or SIM-card to any other person, he or she—

a. must, if the receiver of that cellular phone or SIM-card is a natural person—

(i) obtain from him or her—

(aa) his or her full names, identity number, residential and business or postal address, whichever is applicable; and

(bb) a certified photocopy **[of that page]** of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear **[and must]**;

(ii) retain **[such]** the photocopy obtained in terms of subparagraph (i)(bb); and

[(ii)](iii) verify the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; or

b. must, if the receiver of that cellular phone or SIM-card is a juristic person—

i. obtain from the person representing that juristic person—

(aa) his or her full names, identity number, residential and postal address, whichever is applicable;

(bb) the business name and address and, if registered as such in terms of any law, the registration number of that juristic person;

(cc) a certified photocopy **[of that page]** of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear; and

(dd) a certified photocopy of the business letterhead of, or other similar document relating to, that juristic person;

ii. retain the photocopies obtained in terms of subparagraph (i)(cc) and (dd); and

iii. verify—

(aa) the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; and

(bb) the name and registration number of that juristic person with reference to its business letterhead or other similar document; and

c. may obtain from the receiver of that cellular phone or SIM-card any other information which the person who sells or in any other manner provides the cellular phone or SIM-card deems necessary for purposes of this Act.

(2) Section 39(2), (3) and (4) applies, with the necessary changes, in respect of any person who sold, or in any other manner provided, a cellular phone or SIM-card to any other person.

Loss, theft or destruction of cellular phone or SIM-card to be reported

41. (1) Whenever a cellular phone or SIM-card is lost, stolen or destroyed, the owner of that cellular phone or SIM-card, or any other person who was in possession, or had control, thereof when it was so lost, stolen or destroyed, must within **[24 hours]** a reasonable time after having reasonably become aware of the loss, theft or destruction of the cellular phone or SIM-card, report such loss, theft or destruction in person or through a person authorized thereto by him or her, to a police official at any police station.

(2) A police official who receives a report contemplated in subsection (1), must immediately provide the person who makes the report with written proof that the report has been made or, in the case of a telephonic report, with the official reference number of the report.

(3) A record of every report made in terms of subsection (1) must be kept at the police station where such a report has been made.

(4) (a) The Minister must, within three months after the fixed date and in consultation with the Minister for Safety and Security, issue

directives prescribing—

i. the form and manner in which—

(aa) a report contemplated in subsection (1) must be made; and
(bb) records contemplated in subsection (3) must be kept; and

ii. the information to be contained in such a report or record.

b. Any directive issued under paragraph (a) may at any time in like manner be amended or withdrawn.

c. Any directive issued under paragraph (a) must, before the implementation thereof, be submitted to Parliament.

CHAPTER 8

GENERAL PROHIBITIONS AND EXEMPTIONS

Prohibition on disclosure of information

42. (1) No person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this 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; or

d. to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) No—

a. postal service provider, telecommunication service provider or decryption key holder may disclose any information which he or she obtained in the exercising 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 decryption 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 exercising of any power or the performance of any duty in terms of this Act, whether that employee is involved in the exercising of that power or the performance of that duty or not,

except for the purposes mentioned in subsection (1).

[(3) No otherwise privileged communication intercepted, or archived or real-time call-related information obtained, under, or in contravention of, this Act shall loose its privileged character.]

(3) The information contemplated in subsections (1) and (2) includes information relating to the fact that—

a. a direction has been issued in terms of this Act;

b. a communication is being or has been or will probably be intercepted;

c. archived or real-time communication-related information is being or has been or will probably be provided;

d. a decryption key is being or has been or will probably be disclosed or that decryption assistance is being or has been or will probably be provided; and

e. an interception device is being or has been or will probably be installed.

Disclosure of information by authorised person for performance of official duties

43. Notwithstanding section 42(1), any authorised person who executes a direction or assists with the execution thereof and who has obtained knowledge of—

a. the contents of any communication intercepted under that direction, or evidence derived therefrom; or

b. archived or real-time communication-related information provided under that direction,

may—

i. disclose such contents or evidence or archived or real-time communication-related information to another law enforcement officer, to the extent that such disclosure is **[appropriate to]** necessary for the proper performance of the official duties of the authorised person making or the law enforcement officer receiving the disclosure; or

ii. use such contents or evidence or archived or real-time communication-related information to the extent that such use is **[appropriate to]** necessary for the proper performance of his or her official duties.

Listed equipment

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

b. A notice issued under paragraph (a) may at any time in like manner be amended or withdrawn.

c. The first notice to be issued under paragraph (a) must be published in the *Gazette* within three months after the fixed date.

(2) (a) Before the Minister exercises the powers conferred upon him or her by subsection (1), he or she must—

i. consult the relevant Ministers; and

ii. cause to be published in the *Gazette* a draft of the proposed notice, together with a notice inviting all interested parties to submit to him or her in writing and within a specified period, comments and representations in connection with the proposed notice.

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

(3) Subsection (2) does not apply —

a. if the Minister, in pursuance of comments and representations received in terms of subsection (2)(a)(ii), decides to publish a notice referred to in subsection (1) in an amended form; and

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

(4) Any notice issued under subsection (1) must, before publication thereof in the *Gazette*, be submitted to Parliament.

Prohibition on manufacture, possession and advertising of listed equipment

44. (1) Subject to subsection (2) and section 46, no person may manufacture, assemble, possess, sell, purchase or advertise any listed equipment.

(2) Subsection (1) does not apply to**[—**

a. any authorised person or the National Director who possesses listed equipment for purposes of using it in the execution of an interception direction or in assisting with the execution thereof; or

b. **]** any telecommunication service provider or other person or the Police Service, Defence Force, Agency, Service or prosecuting authority who manufactures, assembles, possesses, sells, purchases or advertises listed equipment under the authority of a certificate of exemption issued to him or her for that purpose by the Minister under section 46.

Exemptions

44. (1) (a) The Minister may, upon application and in consultation with the relevant Ministers, exempt **[any]**—

[(a)](i) any Internet service provider from complying with section 30(4) in respect of the facilities and devices referred to in section 30(2)(a)(ii); **[or]**

[(b)](ii) any telecommunication service provider or any other person from one or all of the prohibited acts referred to in section 45(1); or

(iii) the Police Service, Defence Force, Agency, Service or prosecuting authority from the prohibited acts of possessing and purchasing referred to in section 45(1),

for such period and on such conditions as the Minister**[, in consultation with the relevant Ministers, determines, including a]**.

(b) A condition referred to in paragraph (a) may include that an Internet service provider to whom exemption has been granted under paragraph (a)(i) must pay as an annual contribution to the Fund such amount as the Minister determines in each case.

(2) The Minister may only grant an exemption under subsection (1)(a) if he or she**[, in consultation with the relevant Ministers,]** is satisfied that—

a. in the case of an exemption under subsection (1)(a)(i), the Internet service provider concerned carries on such a small business that he or she cannot comply with section 30(4); **[and]**or

b. the listed equipment in respect of which the application for exemption is made will be manufactured, assembled, possessed, sold, purchased or advertised for a lawful purpose; and

c. such exemption is in the public interest; or

d. special circumstances exist which justify such exemption.

[(3) The Minister must, in considering an application for exemption under subsection (1), take all relevant factors into account, including in the case of an application for exemption under—

a. subsection (1)(a), the total—

i. full-time equivalent of paid employees;

ii. annual turn-over;

iii. gross asset value; and

iv. number of customers,

of the Internet service provider concerned; and

b. subsection (1)(b)—

i. if the application is made by a person other than a telecommunication service provider, the kind of business which that person carries on or intends to carry on; and

ii. the purposes for which the listed equipment in respect of which the application for exemption is made will be manufactured, assembled, possessed, sold, purchased or advertised.]

(3) (a) An exemption under subsection (1)(a) must be granted by issuing to the—

(i) Internet service provider concerned;
(ii) telecommunication service provider or other person concerned; or
Police Service, Defence Force, Agency, Service or prosecuting authority,

a certificate of exemption in which his or her or its name and the scope, period and conditions of the exemption are specified.

b. A certificate of exemption issued in terms of paragraph (a)—

i. must be published in the *Gazette*; and

ii. becomes valid upon the date of such publication.

(4) (a) The Minister must, before he or she **[issues]** publishes a certificate of exemption in terms of subsection (3)(b)(i), table such certificate in draft form in Parliament for approval.

b. Parliament may reject a certificate tabled in terms of paragraph (a) within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its next ensuing ordinary session.

c. If Parliament rejects such a certificate, the Minister **[must—**

i. withdraw that certificate; or

ii. **]** may table an amended certificate in draft form in Parliament.

d. If the Minister tables an amended certificate and Parliament—

i. approves the amended certificate, the Minister must **[issue]** publish that certificate in terms of subsection (3)(b)(i) within one month of Parliament's approval; or

ii. rejects the amended certificate within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its next ensuing ordinary session, paragraph (c) and this paragraph apply.

e. If Parliament does not reject a certificate as contemplated in paragraph (b) or (d)(ii)—

i. such certificate will be deemed to have been approved by Parliament; and

ii. the Minister must publish that certificate in terms of subsection (3)(b)(i) within one month thereafter.

(5) A certificate of exemption contemplated in subsection (3) may at any time in like manner be amended or withdrawn by the Minister.

(6) An exemption under subsection (1)(a) lapses upon—

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

b. withdrawal of the relevant certificate under subsection (5).

(7) If exemption has been granted to an Internet service provider under subsection (1)(a)(i)—

a. that Internet service provider will be subject to all the other applicable provisions of this Act; and

b. the Police Service, the Defence Force, the Agency, the Service, the Directorate or the National Director, whichever made the application for the issuing of the direction which is addressed to such Internet service provider, must make available the necessary facilities and devices to execute that direction.

CHAPTER 9

CRIMINAL PROCEEDINGS, OFFENCES AND PENALTIES

Use of information in criminal proceedings

47. (1) Information regarding the commission of any criminal offence, obtained by means of any interception, or the provision of any archived or real-time communication-related information, under this Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) Any information obtained by the application of this Act, or any similar Act in another country, may only be used as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, with the written authority **[permission/consent]** of the National Director, or any member of the prosecuting authority authorised thereto in writing by the National Director.

[(3) The contents of any communication that is obtained by means of any interception under section 9(1) are inadmissible as evidence in any criminal proceedings, except for the purposes of criminal proceedings in which actual, attempted or threatened bodily harm *{or serious damage to property}* is alleged.]

Proof of certain facts by certificate

48. Whenever in any criminal proceedings or civil proceedings in terms of Chapter 5 or 6 of the Prevention of Organised Crime Act, the question arises whether a designated judge, judge of a High Court, regional magistrate or magistrate has issued a direction under this Act, a certificate signed by a designated judge, judge of a High Court, regional magistrate or magistrate in which he or she–

a. alleges that he or she has received and considered an application made to him or her in terms of this Act;

b. alleges that he or she has issued a direction under this Act; and

c. specifies the contents of such direction,

shall, upon its mere production at such proceedings, be *prima facie* proof that the designated judge, judge of a High Court, regional magistrate or magistrate concerned received and considered such application, issued such direction and of the contents thereof.

Unlawful interception of communication

49. (1) 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 in the Republic, any communication in the course of its occurrence or transmission, is guilty of an offence.

(2) Subsection (1) does not apply to the interception of a communication in terms of sections 3, 4, 5, 6, 7, 8, 9 and 10.

Unlawful provision of archived or real-time communication-related information

50. (1) Any telecommunication service provider or employee of a telecommunication service provider who provides or attempts to provide any archived or real-time communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such archived or real-time communication-related information relates, is guilty of an offence.

(2) Subsection (1) does not apply to the provision of archived or real-time communication-related information in terms of sections 13, 14 and 15.

Offences and penalties

51. (1) (a) Any person who—

i. contravenes or fails to comply with section **[2,]** 9(2), 8(2) or (3), 29(8), 40, **[39(1)]**, 42(1) or 45(1);

ii. in any application made in terms of this Act, furnishes information or makes a statement, knowing such information or statement to be false, incorrect or misleading or not believing it to be correct;

iii. acts contrary to the authority of any direction issued under this Act or proceeds to act under any such direction knowing that it has expired;

iv. acts contrary to the authority of an entry warrant issued under this Act or, without being authorised thereto under an entry warrant, enters any premises for a purpose referred to in the definition of "entry warrant";

v. forges or, with the intent to deceive, **[forges,]** alters or tampers with any direction or entry warrant issued under this Act;

vi. furnishes particulars or information in any affidavit or report referred to in this Act, knowing such particulars or information to be false, incorrect or misleading or not believing it to be correct;

vii. obstructs **[or]**, hinders or interferes with an authorised person who executes any direction or entry warrant issued under this Act or assists with the execution thereof, in the exercising of his or her powers under that direction or entry warrant; or

viii. otherwise than in accordance with, or in a manner allowed by, this Act, authorises or procures any person to intercept any communication or authorises or procures any telecommunication service provider or employee of a telecommunication service provider to provide any archived or real-time communication-related information to him or her or any other person, is guilty of an offence.

b. Any person who is convicted of an offence referred to in paragraph (a) or in section 49, 52, 53(1), 54 or 55(1), is liable to a fine or to imprisonment for a period not exceeding 20 years.

(2) (a) Any postal service provider or employee of a postal service provider who—

i. contravenes or fails to comply with section 28(1)(a);

ii. contravenes or fails to comply with section 42(2); or

iii. performs an act contemplated in subsection (1)(a)(iii), (v) or (vii), is guilty of an offence.

b. Any postal service provider or employee of a postal service provider who is convicted of an offence referred to in paragraph (a) is liable, in the case of—

i. a postal service provider who is a—

(aa) natural person, to a fine or to imprisonment for a period not exceeding 20 years; or
(bb) juristic person, to a fine not exceeding R2, 000 000; or

ii. an employee, to a fine or to imprisonment for a period not exceeding 20 years.

(3) (a) Any telecommunication service provider or employee of a telecommunication service provider who—

i. contravenes or fails to comply with section 28(1)(b) or (2), 30(1) or 39(3);

ii. contravenes or fails to comply with section 30(4);

iii. contravenes or fails to comply with section **[3,]** 6(5), 7(5), 39(1) or (2) or 42(2); or

iv. performs an act contemplated in subsection (1)(a)(iii), (v) or (vii), is guilty of an offence.

b. Any telecommunication service provider or employee of a telecommunication service provider who is convicted of an offence referred to in paragraph (a) or in section 50, is liable, in the case of—

i. a telecommunication service provider who is a—

(aa) natural person, to a fine or to imprisonment for a period not exceeding 20 years; or
(bb) juristic person, to a fine not exceeding R2, 000 000; or

ii. an employee, to a fine or to imprisonment for a period not exceeding 20 years.

(4) (a) Any decryption key holder or any employee of a decryption key holder who—

i. contravenes or fails to comply with section 29(1);

ii. contravenes or fails to comply with section 29(2), (3)(b), (5) or (7) or 42(2); or

iii. performs an act contemplated in subsection (1)(a)(iii), (v) or (vii),

is guilty of an offence.

b. Any decryption key holder or employee of a decryption key holder who is convicted of an offence referred to in paragraph (a) is liable, in the case of—

i. a decryption key holder who is a—

(aa) natural person, to a fine or to imprisonment for a period not exceeding 20 years; or
(bb) juristic person, to a fine not exceeding R2, 000 000; or

ii. an employee, to a fine or to imprisonment for a period not exceeding 20 years.

(5) (a) Any person, including a postal service provider, telecommunication service provider or decryption key holder, who contravenes or fails to comply with any provision of this Act, or any direction, directive, certificate or exemption issued or granted under this Act is, if any such contravention or failure is not declared an offence in terms of any other provision of this section, guilty of an offence.

b. Any person, postal service provider, telecommunication service provider or decryption key holder who is convicted of an offence referred to in paragraph (a) is liable, in the case of—

i. a person or a postal service provider, telecommunication service provider or decryption key holder who is a natural person, to a fine or to imprisonment for a period not exceeding 20 years; or

ii. a postal service provider, telecommunication service provider or decryption key holder who is a juristic person, to a fine not exceeding R2, 000 000.

(6) A conviction of an offence referred to in—

a. subsection (2)(a)(i) does not relieve any postal service provider or any employee of such a postal service provider, of the obligation to comply with section 28(1)(a);

b. subsection (3)(a)(i) or (ii) does not relieve any telecommunication service provider or any employee of such a telecommunication service provider, of the obligation to comply with section 28(1)(b) or (2), 30(1) or (4) or 39(3); or

c. subsection (4)(a)(i) does not relieve any decryption key holder or any employee of such a decryption key holder, of the obligation to comply with section 29(1), as the case may be, and the postal service provider, telecommunication service provider or decryption key holder or employee concerned is liable, in the case of—

i. a postal service provider, telecommunication service provider or decryption key holder, as the case may be, who is a—

(aa) natural person, to a further fine not exceeding R10 000; or
(bb) juristic person, to a further fine not exceeding R50 000; or

ii. an employee, to a further fine not exceeding R10 000, for every day during which such contravention or failure continues.

(7) Notwithstanding anything to the contrary in any other law contained, a magistrate's court may impose any penalty provided for in this Act.

(8) No person who—

a. in good faith assists an authorised person with the execution of a direction; and

b. believes on reasonable grounds that such authorised person is acting in accordance with such a direction,is liable to prosecution for a contravention of section 2 or 12.

Failure to give satisfactory account of possession of cellular phone or SIM-card

52. Any person who is found in possession of any cellular phone or SIM-card in regard to which there is reasonable suspicion that it has been stolen and is unable to give a satisfactory account of such possession, is guilty of an offence.

Absence of reasonable cause for believing cellular phone or SIM-card properly acquired

53. (1) Any person who in any manner acquires or receives into his or her possession from any other person a stolen cellular phone or SIM-card without having reasonable cause for believing at the time of such acquisition or receipt that such cellular phone or SIM-card is the property of the person from whom he or she acquires or receives it or that such person has been duly authorized by the owner thereof to deal with it or dispose of it, is guilty of an offence.

(2) In the absence of evidence to the contrary which raises a reasonable doubt, proof of such possession is sufficient evidence of the absence of reasonable cause.

Unlawful acts in respect of telecommunication and other equipment

54. (1) Any person who, intentionally and without just cause, in any manner—

a. modifies, tampers with, alters, reconfigures or interferes with, any telecommunication equipment, including a cellular phone and a SIM-card, or any part thereof;

b. reverse engineer, decompiles, disassembles or interferes with, the software installed on any telecommunication equipment, including a cellular phone and a SIM-card, by the manufacturer thereof; or

c. allows any other person to perform any of the acts referred to in paragraph (a) or (b),

for purposes of circumventing the provisions of this Act, is guilty of an offence.

(2) Any person who, intentionally and without just cause, in any manner—

a. modifies, tampers with or interferes with, any interception or monitoring equipment, device or apparatus installed or utilised in terms of this Act; or

b. allows any other person to perform any of the acts referred to in paragraph (a), is guilty of an offence.

Failure to report loss, theft or destruction of cellular phone or SIM-card and presumption[s relating to failure to report]

55. (1) Any person who fails to report the loss, theft or destruction of a cellular phone or SIM-card in terms of section 41(1), is guilty of an offence.

(2) Whenever a person is charged with an offence **[in terms of this Act of failing to report the loss, theft or destruction of a cellular phone or SIM-card]** referred to in subsection (1) and it is proved that such person was, at the time, the owner or authorised possessor of the cellular phone or SIM-card alleged to have been lost, stolen or destroyed, proof that the person has failed to produce such cellular phone or SIM-card within seven days of a written request by a police official to do so, will, in the absence of evidence to the contrary which raises reasonable doubt, be sufficient evidence that the cellular phone or SIM-card has been lost, stolen or destroyed.

Forfeiture of listed equipment

56. **[(2)]**(1) A court convicting a person of an offence referred to in section 51 must, in addition to any penalty which it may impose in respect of that offence, declare any listed equipment—

a. by means of which the offence was committed;

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

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

d. the possession of which constituted the offence,

to be forfeited to the State**[if no telecommunication service provider or other person has been exempted, under section 44(1), from one or all of the prohibited acts referred to in section 43(1) in respect of such listed equipment]**.

[(1)](2) A court convicting a person of an offence referred to in section 51 may, in addition to any penalty which it may impose in respect of that offence, declare any **[listed equipment or other]** equipment, other than listed equipment—

a. by means of which the offence was committed;

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

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

d. the possession of which constituted the offence,

to be forfeited to the State **[if—**

i. **any telecommunication service provider or other person has been exempted, under section 44(1), from one or all of the prohibited acts referred to in section 43(1) in respect of such listed equipment; or**

ii. **such equipment has not been declared to be listed equipment under section 42(1)]**.

[(4)](3) Any listed equipment or other equipment declared forfeited under subsection (1) or (2) must, as soon as practicable after the date of declaration of forfeiture, be delivered to the Police Service.

[(5)](4) Any listed equipment or other equipment delivered to the Police Service in terms of subsection **[(4)]**(3) must, in the case of—

a. listed equipment **[or other equipment]** declared forfeited under subsection (1), be kept by the Police Service —

i. for a period of **[30 days]** three months with effect from the date of declaration of forfeiture; or

ii. if an application is within that period received from any telecommunication service provider or other person for the determination of **[any right referred to in subsection (6)(a)]** the matters referred to in subsection (6)(a), until a final decision in respect of any such application has been given,

and must—

(aa) as soon as practicable after the expiry of the period referred to in subparagraph (i); or
(bb) if the decision referred to in subparagraph (ii) has been given against the telecommunication service provider or other person concerned, as soon as practicable after that decision has been given; or

b. **[listed]** equipment declared forfeited under subsection (2), **[as soon as practicable after receipt thereof]** be kept by the Police Service—

i. for a period of 30 days with effect from the date of declaration of forfeiture; and

ii. must as soon as practicable after the expiry of the period referred to in subparagraph (i),

be destroyed by the Police Service.

[(3)](5) A declaration of forfeiture under subsection (1) does not affect any right **[referred to in subsection (6)(a)]** which any telecommunication service provider or other person, other than the convicted person, may have to such listed equipment **[or other equipment]**, if it is proved that such telecommunication service provider or other person—

a. has been exempted, under section 46(1), from the relevant prohibited act referred to in section 45(1) in respect of such listed equipment;

b. could not reasonably be expected to have known or had no reason to suspect that the listed equipment **[or other equipment]** concerned was being or would be used in connection with the offence; and

c. had taken all reasonable steps to prevent the use thereof in connection with the offence**[; or**

d. **could not have prevented the commission of the offence]**.

(6) (a) The court in question or, if the judge or judicial officer concerned is not available, any other judge or judicial officer of the court in question, may at any time within a period of three **[years]** months with effect from the date of declaration of forfeiture under subsection (1), upon the application of any telecommunication service provider or other person, other than the convicted person, who claims that—

i. the listed equipment declared forfeited under subsection (1) is his or her property; and

ii. he or she is a person referred to in subsection (5),

inquire into and determine those matters.

b. If the court referred to in paragraph (a) is satisfied that—

i. the listed equipment concerned is the property of the telecommunication service provider or other person concerned; and

ii. the telecommunication service provider or other person concerned is a person referred to in subsection (5),

the court must set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to such telecommunication service provider or other person.

[any right referred to in subparagraph (i) or (ii) is vested in him or her, inquire into and determine any such right, and if the court *{finds / is satisfied}* that the listed equipment or other equipment concerned—

i. is the property of any such telecommunication service provider or other person, the court must—

(aa) set aside the declaration of forfeiture and direct that the listed equipment or other equipment concerned be returned to such telecommunication service provider or other person; or

(bb) if the State has disposed of the listed equipment or other equipment concerned, direct that such telecommunication service provider or other person be compensated by the State to an amount equal to the value of that listed equipment or other equipment; or

ii. was sold to the convicted person by such telecommunication service provider or other person in pursuance of a contract under which the convicted person becomes the owner of such listed equipment or other equipment, upon the payment of a stipulated price, whether by instalments or otherwise, and under which the telecommunication service provider or other person concerned becomes entitled to the return of such listed equipment or other equipment upon default of payment of the stipulated price or any part thereof, the court must—

(aa) direct that the listed equipment or other equipment concerned be returned to the telecommunication service provider or other person concerned; or

(bb) if the State has disposed of the listed equipment or other equipment concerned, direct that the telecommunication service provider or other person concerned be compensated by the State to an amount equal to the value of his or her rights under the contract to the listed equipment or other equipment concerned.]

[(b)](c) If a determination by the court under paragraph **[(a)]**(b) is adverse to the applicant, he or she may appeal therefrom as if it were a conviction by the court making the determination, and such appeal may be heard either separately or jointly with an appeal against the conviction as a result whereof the declaration of forfeiture under subsection (1) was made, or against a sentence imposed as a result of such conviction.

c. (c) When determining **[any rights under this subsection]** the matters referred to in paragraph (a)(i) and (ii), the record of the criminal proceedings in which the declaration of forfeiture under subsection (1) was made, must form part of the relevant proceedings, and the court making the determination may hear such additional evidence, whether by affidavit or orally, as it

deems fit.

Revoking of licence to provide telecommunication service

57. The Minister of Communications, after consultation with the **[Independent Communications Authority of South Africa, established by section 3 of the Independent Communications Authority of South Africa Act, 2000 (Act No. 13 of 2000)]** Authority, may, in the case of a second or subsequent conviction of a telecommunication service provider of an offence referred to in section 51(3)(a)(ii) and notwithstanding the imposition of any penalty prescribed by section 51(3)(b) and (6), revoke the licence issued to the telecommunication service provider concerned under Chapter V of the Telecommunications Act, to provide a telecommunication service.

CHAPTER 10

GENERAL PROVISIONS

Supplementary directives regarding applications

58. (1) A designated judge or, if there is more than one designated judge, all the designated judges jointly, may, after consultation with the respective Judges-President of the High Courts, issue directives to supplement the procedure for making applications for the issuing of directions or entry warrants in terms of this Act.

(2) Any directive issued under subsection (1) may at any time in like manner be amended or withdrawn.

(3) Any directive issued under subsection (1) must be submitted to Parliament.

Amendment of section 205 of Act 51 of 1977, as substituted by section 11 of Act 204 of 1993

[17]59. Section 205 of the Criminal Procedure Act, 1977, is hereby amended by the substitution for subsection (1) of the following subsection:

"(1) A judge of **[the supreme court]** a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the Regulation of Interception of Communications Act, 2002, upon the request of **[an attorney-general]** a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the **[attorney-general]** Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for examination by the **[attorney-general]** Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the **[attorney-general]** Director of Public Prosecutions, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the **[attorney-general]** Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.".

Amendment of section 11 of Act 140 of 1992

[18]60. Section 11 of the Drugs and Drug Trafficking Act, 1992, is hereby amended by the substitution in subsection (1) for paragraph *(e)* of the following paragraph:

"*(e)* subject to section 15 of the Regulation of Interception of Communications Act, 2002, require from any person who has in his or her possession or custody or under his or her control any register, record or other document which in the opinion of the police official may have a bearing on any offence or alleged offence under this Act, to deliver to him or her then and there, or to submit to him or her at such time and place as may be determined by the police official, any such register, record or document;".

[Amendment of section 5 of Act 38 of 1994, as amended by section 5 of Act 66 of 2000

[19]58. Section 5 of the Intelligence Services Act, 1994, is hereby amended—

a. by the substitution in subsection (2) for the words preceding paragraph *(a)* of the following words:

"If a judge as defined in section 1 of the Regulation of Interception [and Monitoring Prohibition] of Communications Act, [1992 (Act No. 127 of 1992)] 2002, is [convinced] satisfied, on the [grounds mentioned] facts alleged in a written application complying with directives issued under subsection (7), that there are reasonable grounds to believe that—";

b. by the substitution in subsection (3) for paragraph *(a)* of the following paragraph:

"*(a)* A direction referred to in subsection (2) shall be issued by the judge concerned for a specific period not exceeding three months at a time, and the period for which it has been issued shall be mentioned in the direction.";

c. by the substitution for subsection (4) of the following subsection:

"(4) The judge referred to in subsection (2) may, upon a written application complying with the directives issued under subsection (7)—

***(a)* extend the period referred to in subsection (3) for a further period not exceeding three months at a time; or**

***(b)* amend an existing direction referred to in subsection (3),**

if that judge is [convinced] satisfied that the extension or, amendment, as the case may be, is necessary for a

reason mentioned in subsection (2)."; and

d. by the substitution for subsection (7) of the following subsection:

"(7) *(a)* The Judges-President of the [several Divisions of the Supreme Court of South Africa] High Courts may jointly issue directives to uniformly regulate the manner and procedure of applications in terms of subsection (2).

***(b)* If the judge referred to in subsection (2) considers any case to be sufficiently urgent, the procedure contemplated in paragraph *(a)* may be dispensed with and the matter may be dealt with in such manner and subject to such conditions as he or she deems fit, including, in an appropriate case, the hearing of an oral application and the granting of an oral direction.**

***(c)* An oral direction referred to in paragraph *(b)* must be confirmed in writing within 48 hours.".]**

Amendment of section 3 of Act 40 of 1994, as amended by section 3 of Act 31 of 1995 and section 3 of Act 42 of 1999

61. **[20]** Section 3 of the Intelligence Services Control Act, 1994, is hereby amended by the substitution in paragraph *(a)* for subparagraph (iii) of the following subparagraph:

"(iii) any designated judge as defined in section 1 of the Regulation of Interception **[and Monitoring Prohibition]** of Communications Act, **[1992 (Act No. 127 of 1992)]** 2002, a report regarding the functions performed by him or her in terms of that Act, including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate: Provided that such report shall not disclose any information contained in an application or direction **[contemplated in section 3 of]** referred to in that Act;".

Repeal of law and transitional arrangements

62. (1) Subject to subsections (2) and (3), the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), is hereby repealed.

(2) Any judge whose designation in terms of the Interception and Monitoring Prohibition Act, 1992, to perform the functions of a judge for purposes of that Act **[was]** is still in force **[immediately before]** on the fixed date, must be regarded as having been so designated in terms of this Act.

(3) A direction issued under section 3 of the Interception and Monitoring Prohibition Act, 1992, and which is still in force **[immediately before]** on the fixed date, must be regarded as having been issued under this Act and remains in force until the period or extended period for which that direction has been issued, lapses.

[(4) Any—

a. information which has been obtained as contemplated in section 5, 6 or 12; and

b. communication-related information which has been obtained as contemplated in section 15 or 16,

before the fixed date, is admissible as evidence in any criminal proceedings as if those provisions were in operation at the date of obtaining such information.]

[(5)](4) The directives issued in terms of section 6 of the Interception and Monitoring Prohibition Act, 1992, and which are still in force immediately before the fixed date, cease to be of force and effect from the fixed date.

Short title *{[and commencement]}*

63. This Act is called the Regulation of Interception of Communications Act, 2002 ***{[, and comes into operation on a date fixed by the President by proclamation in the Gazette]}***.

SCHEDULE

(Section 1)

1. high treason;
2. sedition;
3. any offence relating to terrorism;
4. any offence involving sabotage;
5. any offence which could result in the loss of a person's life or serious risk of loss of a person's life;
6. any offence referred to in Schedule 1 to the Implementation of the Rome Statute of the International Criminal Court Act, 2002 (Act No. 27 of 2002);
7. any specified offence as defined in section 1 of the National Prosecuting Authority Act;
8. any offence referred to in Chapters 2, 3 and 4 of the Prevention of Organised Crime Act;

9. any offence referred to in section 13(f) of the Drugs and Drug Trafficking Act, 1992 (Act No. 140 of 1992);

10. any offence relating to the dealing in or smuggling of ammunition, firearms, explosives or armament and the unlawful possession of such firearms, explosives or armament;

11. any offence under any law relating to the illicit dealing in or possession of precious metals or precious stones;

12. any offence contemplated in *{**[section 1(1) of the Corruption Act, 1992 (Act No. 94 of 1992)]** / the Prevention of Corruption Act, 2002}*;

13. dealing in, being in possession of or conveying endangered, scarce and protected game or plants or parts or remains thereof in contravention of **[a statute or provincial ordinance]** any legislation;

14. any offence the punishment wherefor may be imprisonment for life or a period of imprisonment exceeding **[7 / 10]** five years without the option of a fine.