(8) If a period of more than three years has been determined in terms of subsection (2)*(a)*(iii), the Cabinet member responsible for communications may, upon application by the telecommunication service provider concerned and in consultation with the relevant Ministers, reduce that period to a period which may not be less than three years by issuing an amended directive under subsection (2)*(a)*.

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

31. (1) *(a)* The Minister, after consultation with the Cabinet members responsible for communications and national financial matters 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 compensated; and

(ii) reasonable tariffs of 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(c) A notice issued under paragraph *(a)* may at any time in like manner be amended or withdrawn.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 making available of a facility, device or telecommunication system; and

(b) decryption key holder, the—

(i) disclosure of a decryption key; and

(ii) provision of decryption assistance.

(3) The compensation payable to a postal service provider, telecommunication service provider or decryption key holder in terms of this section will only be for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance contemplated in subsection (1)*(a)*(i).

(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 INTERNET SERVICE PROVIDERS ASSISTANCE FUND

Establishment of interception centres

32. (1) The Minister, in consultation with the relevant Ministers and the Cabinet member responsible for national financial matters, must, at State expense—

(a) establish one or more centres, to be known as interception centres, for the interception of communications in terms of this Act;

(b) equip, operate and maintain such interception centres;

(c) acquire, install and maintain connections between telecommunication systems and interception centres; and

(d) administer the interception centres.

(2) The Minister must exercise final responsibility over the administration and functioning of interception centres.

(3) Notwithstanding the Telecommunications Act, 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 that Act; and

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

(4) The Minister must enter into service level agreements with the relevant Ministers in respect of the provision of services by the interception centres to the law enforcement agencies.

(5) The Executive Director may enter into agreements with the National Commissioner and National Director to make use of the services of interception centres, including the cost thereof.

Establishment of Office for Interception Centres

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

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 as the 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 Office as Acting Director, to exercise the powers, perform the functions and carry out the duties of the Director.

(4) 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 law enforcement agencies, seconded or designated to the Office for that purpose by the—
  (i) National Commissioner;
  (ii) Secretary for Defence;
  (iii) Director-General: National Intelligence Agency;
  (iv) Director-General: South African Secret Service; and
  (v) National Director; and

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

(5) A member or an officer may only be seconded or designated as contemplated in this section and section 36—

(a) in terms of the laws regulating such secondment;

(b) with his or her consent; and

(c) after a security clearance has been issued by the Agency in respect of that member or officer.

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 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;

(g) must prescribe the manner in, and the period for, which such information must be kept; and

(h) 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, accountable to the Minister.

(2) A member or an officer seconded or designated in terms of section 34(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, subject to the control and directions of the Director.

(3) The law enforcement agencies 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)*(a)*, request the persons referred to in section 34(4)*(a)*(i) to (v) to second a member or an officer 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 or an officer as head of an interception centre is pending, the Minister may request the persons referred to in section 34(4)*(a)*(i) to (v), to designate, from among their respective Departments, a member or an officer to 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—

(a) members of the law enforcement agencies, seconded or designated to the interception centre concerned for that purpose by the persons referred to in section 34(4)*(a)*(i) to (v); and

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

(5) A member or an officer seconded or 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 centre concerned.

(6) In order to achieve the objects of this Act, the head of an interception centre must exercise control over members and officers seconded or designated to 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)*(f)*.

(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 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 centre 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 Internet Service Providers Assistance Fund

38. (1) There is hereby established a fund to be known as the 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, in consultation with the relevant Ministers, under the control and management of the Director, who—

(a) must utilise 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) The Minister, in consultation with the relevant Ministers, 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 Cabinet member responsible for national financial matters, 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 providers

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 his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear;

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

(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 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 the—

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

(bb) 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;

(b) the telephone number or any other number allocated to the person concerned; and

(c) 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.

(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 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 immediately 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 his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear;

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

(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 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 the—
(aa) photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; and
(bb) 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) A person 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;
(b) the cellular telephone number or any other number allocated to the other person;
(c) the number of the cellular phone concerned; and
(d) any other information in respect of the other person which the person concerned may require in order to enable him or her to identify that other person.

(3) Section 39(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 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 authorised 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 Cabinet member responsible for policing, issue directives prescribing the—
(i) 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) 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) The information contemplated in subsections (1) and (2) includes information relating to the fact that—

(a) a direction has been issued under this Act;

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

(c) real-time or archived 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) real-time or archived communication-related information provided under that direction,

may—

(i) disclose such contents or evidence or real-time or archived communication-related information to another law enforcement officer, to the extent that such disclosure is 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 real-time or archived communication-related information to the extent that such use is 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 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

45. (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 any telecommunication service provider or other person who, or law enforcement agency which, manufactures, assembles, possesses, sells, purchases or advertises listed equipment under the authority of a certificate of exemption issued to him or her or it for that purpose by the Minister under section 46.

Exemptions

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

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

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

(iii) law enforcement agency from the prohibited acts of possessing and purchasing referred to in section 45(1),

for such period and on such conditions as the Minister determines.

(b) A condition referred to in paragraph *(a)* may include that an Internet service provider to whom an 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 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); or

(b) in the case of an exemption under subsection (1)*(a)*(ii), the purpose for which the listed equipment will be manufactured, assembled, possessed, sold, purchased or advertised is reasonably necessary; and

(c) such exemption is in the public interest; or

(d) special circumstances exist which justify such exemption.

(3) *(a)* An exemption under subsection (1)*(a)* must be granted by issuing to the—

(i) Internet service provider;

(ii) telecommunication service provider or other person; or

(iii) law enforcement agency,

concerned, 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 under 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 publishes a certificate of exemption in terms of subsection (3)*(b)*(i), table such certificate in the National Assembly for approval.

(b) The National Assembly 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 the National Assembly rejects such a certificate, the Minister may table an amended certificate in the National Assembly.

(d) If the Minister tables an amended certificate and the National Assembly—

(i) approves the amended certificate, the Minister must publish that certificate in terms of subsection (3)*(b)*(i) within one month of the National Assembly'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 the National Assembly does not reject a certificate as contemplated in paragraph *(b)* or *(d)*(ii)—

(i) such certificate will be deemed to have been approved by the National Assembly; 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 an 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 law enforcement agency which 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 real-time or archived 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 of the National Director, or any member of the prosecuting authority authorised thereto in writing by the National Director.

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—

(a) interception of a communication as contemplated in sections 3, 4, 5, 6, 7, 8 and 9; or

(b) monitoring of a signal or radio frequency spectrum as contemplated in sections 10 and 11.

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

50. (1) Any telecommunication service provider or employee of a telecommunication service provider who intentionally provides or attempts to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates, is guilty of an offence.

(2) Subsection (1) does not apply to the provision of real-time or archived communication-related information as contemplated in sections 13, 14 and 15.

Offences and penalties

51. (1) *(a)* Any person who—

(i) contravenes or fails to comply with section 6(2), 7(4), 8(4), 29(8), 40(1), (2) or (3), 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 purposes of intercepting a postal article or communication, or installing and maintaining an interception device, on that premises;

(v) forges or, with the intent to deceive, 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; or

(vii) obstructs, 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,

is guilty of an offence.

(b) Any person who is convicted of an offence referred to in—

(i) paragraph *(a)* or in section 49(1) or 54, is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

(ii) section 52, 53(1) or 55(1), is liable to a fine or to imprisonment for a period not exceeding two 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 not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
(bb) juristic person, to a fine not exceeding R5 000 000; or
(ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

(3) *(a)* Any telecommunication service provider or employee of a telecommunication service provider who—
(i) contravenes or fails to comply with section 7(2), 8(3), 28(1)*(b)* or (2), 30(1) or 39(4);
(ii) contravenes or fails to comply with section 30(4);
(iii) contravenes or fails to comply with section 7(5), 8(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(1), is liable, in the case of—
(i) a telecommunication service provider who is a—
(aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
(bb) juristic person, to a fine not exceeding R5 000 000; or
(ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 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 not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
(bb) juristic person, to a fine not exceeding R5 000 000; or
(ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

(5) 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(4); 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).

(6) Notwithstanding anything to the contrary in any other law contained, a magistrate's court may impose any penalty provided for in this Act.

(7) 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 this Act.

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 authorised 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 unlawfully, 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 engineers, 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)*,

is guilty of an offence.

(2) Any person who, intentionally and unlawfully, 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

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 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.

Revoking of licence to provide telecommunication service

56. The Cabinet member responsible for communications, after consultation with the 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)*, revoke the licence issued to the telecommunication service provider concerned under Chapter V of the Telecommunications Act, to provide a telecommunication service.

Forfeiture of listed or other equipment

57. (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.

(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 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.

(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.

(4) Any listed equipment or other equipment delivered to the Police Service in terms of subsection (3) must, in the case of—

(a) listed equipment declared forfeited under subsection (1), be kept by the Police Service—
(i) for a period of four months with effect from the date of declaration of forfeiture;
(ii) if an application referred to in subsection (6)*(a)* is made, until a final decision in respect of any such application has been given; or
(iii) if an application referred to in subsection (7)*(a)* is made, 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);
(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
(cc) if an application referred to in subparagraph (iii) has been refused, as soon as practicable after such refusal; or
(b) equipment declared forfeited under subsection (2), 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.

(5) A declaration of forfeiture under subsection (1) does not affect any right which any telecommunication service provider or other person, other than the convicted person, may have to such listed equipment, if it is proved that such telecommunication service provider or other person—

(a) has been exempted, under section 46(1)*(a)*, 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 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.

(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 upon an application made at any time within a period of three months with effect from the date of declaration of forfeiture under subsection (1), by 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 the—

(i) listed equipment concerned is the property of the telecommunication service provider or other person concerned; and

(ii) 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.

(c) If a determination by the court under paragraph *(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.

(d) When determining 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.

(7) *(a)* The Minister may, if an application referred to in subsection (6)*(a)*—

(i) has not been made, upon an application made at any time after a period of three months with effect from the date of declaration of forfeiture under subsection (1) but before the expiry of a period of four months from that date; or

(ii) has been made and the declaration of forfeiture has not been set aside, upon an application made at any time within a period of one month with effect from the date on which a final decision in respect of that application has been given,

in terms of section 46(1)*(a)*(iii) exempt the law enforcement agency which made the application from possessing the listed equipment declared forfeited under subsection (1).

(b) Section 46 applies with the necessary changes in respect of an application referred to in paragraph *(a)*.

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

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 and Provision of Communication-related Information 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

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 and Provision of Communication-related Information 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 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. 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 and Provision of Communication-related Information 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 is still in force 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 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) The directives issued under 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.

(5) *(a)* Any place which, immediately before the fixed date, has been used by the Police Service, Defence Force, Agency, Service or Directorate for the interception and monitoring of communications in terms of the Interception and Monitoring Prohibition Act, 1992, will, as from a date specified by the Cabinet member responsible for intelligence services, cease to exist unless such place is established as an interception centre as contemplated in section 32(1)*(a)*.

(b) If any place referred to in paragraph *(a)*—

(i) is established as an interception centre as contemplated in that paragraph, all assets, liabilities, rights and obligations of that place will vest in the interception centre so established; or

(ii) ceases to exist as contemplated in that paragraph, all—

(aa) assets, including liabilities and obligations relating thereto, and rights of that place will, as from the date on which it ceases to exist, vest in interception centres established by section 32(1)*(a)* and specified by the Cabinet member responsible for intelligence services for that purpose,

without formal transfer and without payment of any fees, duties, taxes or other charges; and

(bb) other liabilities and obligations of that place remain with the Police Service, Defence Force, Agency, Service or Directorate, whichever used that place for purposes referred to in paragraph *(a)*.

(6) *(a)* Any person who, at the fixed date, is the owner of a cellular phone or a SIM-card must, in the manner and within the period determined by the Minister by notice in the *Gazette*, provide the information referred to in section 40(1) to the person who sold, or in any other manner provided, the cellular phone or SIM-card to him or her, or to the telecommunication service provider or other person mentioned in such notice.

(b) Different periods may be determined in terms of paragraph *(a)* in respect of—

(i) owners whose surnames start with different letters of the alphabet, or whose dates of birth fall in different months; or

(ii) categories of numbers of cellular phones or SIM-cards.

(c) Before the Minister exercises the powers conferred on him or her by paragraph *(a)*, he or she must consult the telecommunication service providers concerned.

(d) Any notice issued under paragraph *(a)* must, before publication thereof in the *Gazette*, be submitted to Parliament.

(e) Section 40(2) and (3) applies, with the necessary changes, in respect of a telecommunication service provider or other person to whom information has been provided in terms of paragraph *(a)*.

Short title and commencement

63. This Act is called the Regulation of Interception of Communications and Provision of Communication-related Information 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. any offence relating to terrorism;
3. any offence involving sabotage;
4. sedition;
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);
13. dealing in, being in possession of or conveying endangered, scarce and protected game or plants or parts or remains thereof in contravention of any legislation;
14. any offence the punishment wherefor may be imprisonment for life or a period of imprisonment prescribed by section 51 of the Criminal Law Amendment Act, 1997 (Act No. 105 of 1997), or a period of imprisonment exceeding five years without the option of a fine.

MEMORANDUM ON THE OBJECTS OF THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION BILL

1. BACKGROUND

1.1 Since the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), came into operation on 1 February 1993, there have been considerable technological advances in respect of telecommunications such as cellular, satellite and computer communications through e-mail and the electronic transfer of information and data. There have also been considerable legal developments throughout the world regarding the interception and monitoring of communications. Furthermore, telecommunications are being used increasingly in the organisation and commission of especially organised crime, heists and other serious violent crimes.

1.2 The South African Law Commission, as part of its review of security legislation (Project 105), investigated the subject of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992). The Interception and Monitoring Bill, 2001, as originally introduced in Parliament, emanated from the South African Law Commission's Report on that investigation. The Portfolio Committee on Justice and Constitutional Development (National Assembly), after having considered the above-mentioned Bill and the submissions which it received in respect of that Bill, presented the Regulation of Interception of Communications and Provision of Communication-related Information Bill.

2. OBJECTS OF BILL

2.1 The principal object of the Bill is to regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information.

2.2 Chapter 1 contains a list of definitions and certain introductory provisions.

2.3 Chapter 2 contains general prohibitions of the interception of communications and the provision of communication-related information. However, certain exceptions to those general prohibitions are created, which include, among others, the interception of communications—

* under an interception direction;
* by a party to a communication;
* with the consent of a party to a communication;
* in connection with the carrying on of a business; and
* to prevent serious bodily harm.

2.4 Chapter 3 regulates the making of applications for, and the issuing of—

* directions authorising the interception of communications and the provision of communication-related information; and
* entry warrants authorising entry upon premises for purposes of intercepting postal articles or communications on premises or installing and maintaining interception devices on, and removing interception devices from, premises.

Provision is further made for the cancellation of such directions and entry warrants. Chapter 4 regulates the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders to law enforcement officers executing directions.

2.5 Chapter 5 provides for the interception capability of telecommunication services and the storing of communication-related information by telecommunication service providers. Provision is further made for the facilities and devices to be acquired by telecommunication service providers to enable the interception of indirect communications and the storing of communication-related information. It also regulates the compensation payable to postal service providers, telecommunication service providers and decryption key holders for certain forms of assistance given by them in the execution of directions by law enforcement officers.

2.6 Chapter 6 provides for the establishment, equipping, operation and maintenance of interception centres. Provision is made for the establishment of an Office for Interception Centres and the Internet Service Providers Assistance Fund. It also provides for the secondment of a person to the Office as the Director of the Office and regulates

the powers, functions and duties of the Director. Provision is made for the secondment of persons to interception centres as the heads thereof.

2.7 Chapter 7 imposes certain duties on telecommunication service providers and other persons. Telecommunication service providers are required to obtain and keep certain information in respect of their customers, cellular phones and SIM-cards. It also contains a general obligation to report the loss, theft or destruction of cellular phones or SIM-cards.

2.8 Chapter 8 contains general prohibitions and exceptions thereto. A prohibition is placed on the disclosure of information which is obtained in terms of the Bill. Provision is also made for the declaration of certain instruments, devices or equipment, the design of which renders it primarily useful for purposes of the interception of communications, to be listed equipment. The manufacturing, possession and advertising of such equipment are specifically prohibited. However, certain exemptions in respect of those prohibitions are created.

2.9 Chapter 9 regulates the admissibility and the use of information, obtained by means of interceptions, in criminal proceedings. Certain offences are created and penalties for such offences are prescribed. Some of those offences relate to—

* the unlawful interception of communications;
* the unlawful provision of communication-related information;
* failure to give a satisfactory account of possession of a cellular phone or a SIM-card;
* the absence of reasonable cause for believing that a cellular phone or SIM-card is properly acquired;
* the unlawful acts in respect of telecommunication and other equipment; and
* failure to report the loss, theft or destruction of a cellular phone or SIM-card.

Provision is made for the revoking of licences to provide telecommunication services and for the compulsory forfeiture of listed equipment to the State. Chapter 10 contains general provisions and amendments to other Acts.

3. CONSULTATION PROCESS

The availability of discussion paper 78, which contained provisional recommendations and a draft Bill, was announced at a media conference, as well as on the Law Commission's Website on the Internet, in a Bulletin issued by the Law Commission dated 2 December 1998 and in the *Government Gazette*. The discussion paper was also distributed to approximately 400 local parties and bodies (including Government Departments, law enforcement agencies, telecommunication service providers, individuals and bodies representing the legal community) and to 250 foreign parties and bodies. Written submissions were considered by the Portfolio Committee and public hearings were held.

4. FINANCIAL IMPLICATIONS FOR STATE

While every effort will be made to use existing resources to implement and apply the legislation, there will be financial implications for the State if the legislation is to be implemented successfully, for example in respect of the establishment, equipping, operating and maintenance of interception centres.

5. IMPLICATION FOR PROVINCES

None.

6. PARLIAMENTARY PROCEDURE

The Portfolio Committee and the Department of Justice and Constitutional Development are of the opinion that this Bill must be dealt with in accordance with section 75 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996), since it contains no provision to which the procedure set out in section 74 or 76 of the Constitution applies.