Protection of Communications Secrets Act

up-to-date: Act n. 6626/2002

Article 1 (Purpose)

The purpose of this Act is to protect the secrets of communications and further freedom of communications by confining its objects and requiring it to go through a strict process of law with regard to limitation on secrets and freedom of communications and conversations.

Article 2 (Definitions)

For the purposes of this Act, the definitions of terms shall be as follows: <Amended by Act No. 6546, Dec. 29, 2001>

1. The term "communication" means mail and electronic telecommunications;

2. The term "mail" means ordinary mail and parcel post under the Postal Service Act;

3. The term "telecommnuications" means transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fiber cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging;

4. The term "parties concerned" means senders and addressees of mail, or transmitters and receivers of telecommunications;

5. The term "nationals" means the people of the Republic of Korea who have their addresses or residence in areas where the sovereignty of the Republic of Korea is exercised;

6. The term "censorship" means opening of mail without the consent of the party concerned or acquiring knowledge of, recording or withholding its contents through other means;

7. The term "tapping" means acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception;

8. The term "tapping equipment" means electronic, mechanical or other devices that can be used for tapping conversations or telecommunications: Provided, That those prescribed by the Presidential Decree, from among telecommunications apparatuses and instruments or their parts that are generally used and hearing aids for correcting auditory sense or others used for similar purposes shall be excluded;

9. The term "e-mail" means the transmission of any message or any message transmitted through the computer network;

10. The term "membership information service" means the information service provided to any specific member or contractor, or the network of such information service; and

11.The term "communication confirmation data" means the date of telecommunications by subscribers, the time that the telecommunications commence and end, the number of subscribers and the frequency of use by subscribers, including the number of incoming and outgoing

communications, etc., and the data on the records of telecommunications prescribed by the Presidential Decree.

Article 3 (Protection of Secrets of Communication and Conversation)

(1) No person shall censor any mail, wiretap any telecommunications, provide the communication confirmation data or record or listen to conversations between others that are not made public, without recourse to this Act, the Criminal Procedure Act or the Military Court Act: Provided, That the cases under each of the following subparagraphs shall be determined by the Acts concerned: <Amended by Act No. 6305, Dec. 29, 2000; Act No. 6546, Dec. 29, 2001>

1. Handling of returned mail, etc.: Cases where parcel post (including the similar mail) suspected of containing such contraband items as explosives referred to in Articles 28, 32, 35 and 36 of the Postal Service Act is opened, where the mail cannot be delivered to the addressee or is returned to the sender because of the addressee's refusal to accept it, where the mail is opened in order to identify the address and name of the sender of the mail that the addressee refuses to receive because of missing address and name of the sender, or where any unreturnable mail containing valuable securities is handled;

2. Inspection of import and export mail: Customs clearance of mail other than the letters referred to in Articles 256 and 257 of the Customs Act;

3. Communication with persons under detention or in prison: Control of communication with the persons under detention or in prison as referred to in Article 91 of the Criminal Procedure Act, Article 131 of the Military Court Act, Articles 18 and 19 of the Criminal Administration Act and Articles 15 and 16 of the Military Criminal Administration Act;

4. Communication with bankrupts: Case where a trustee in bankruptcy receives communications addressed to the bankrupt under Article 180 of the Bankruptcy Act; and

5. Monitoring radio waves for the elimination of interference, etc.: Case of monitoring radio waves in order to maintain an order in radio communications by, for example, eliminating interference as referred to in Article 63-2 of the Radio Waves Act.

(2) Any censorship of mail or any wiretapping of telecommunications (hereinafter referred to as "communication-restricting measures") shall be used as a supplementary means of facilitating criminal investigation or ensuring the national security and efforts shall be made to minimize the violation of people's communication secrets. <Newly Inserted by Act No. 6546, Dec. 29, 2001>

Article 4 (Prohibition of Use of Contents of Mail from illegal Inspection and Contents of Telecommunications from Illegal Wiretapping as Evidence)

Mail or its contents obtained through illegal inspection and the contents of communication acquired or recorded through illegal wiretapping in violation of Article 3 shall not be admitted as evidence in a trial or disciplinary procedure.

Article 5 (Requirements for Permission of Communication-Restricting Measures for Criminal Investigation)

(1) The communication-restricting measures shall be allowed only when there is a substantial reason to suspect that a crime under each of the following subparagraphs is being planned or

committed or has been committed, and it is difficult to prevent the committing of the crime, arrest the criminal or collect the evidence: <Amended by Act No. 5454, Dec. 13, 1997; Act No. 6146, Jan. 12, 2000; Act No. 6546, Dec. 29, 2001>

1.Part II of the Criminal Act -- Chapter I Crime concerning Insurrection, crimes provided for in Articles 92 through 101 from among Chapter II Crimes concerning Foreign Aggression, crimes provided for in Articles 107, 108, 111 through 113 from among Chapter IV Crimes concerning Diplomatic Relations, crimes provided for in Articles 114 and 115 from among Chapter V Crimes Harming Public Safety, Chapter VI Crimes concerning Explosives, crimes provided for in Articles 127, 129 through 133 from among Chapter VII Crimes concerning Duties of Public Officials, Chapter IX Crimes of Escape and Sheltering Criminals, crimes provided for in Articles 164 through 167, 172 through 173, 174 and 175 from among Chapter XIII Crimes of Arson and Fire Caused by Negligence, Chapter XVII Crimes concerning Opium, Chapter XVIII Crimes concerning Currency, crimes provided for in Articles 214 through 217, 223 (limited to criminal attempts provided for in Articles 214 through 217) and 224 (limited to preliminary conspiracy provided for in Articles 214 and 215) from among Chapter XIX Crimes concerning Securities, Postage Stamps and Revenue Stamps, Chapter XXIV Crimes of Homicide, Chapter XXIX Crimes of False Arrest and Illegal Confinement, crimes provided for in Articles 283 (1), 284, 285 (limited to habitual criminals provided for in Articles 283 (1) and 284), 286 [limited to attempted criminals provided for in Articles 283 (1), 284, 285 (limited to habitual criminals provided for in Articles 283 (1) and 284)] from among Chapter XXX Crimes of Intimidation, Chapter XXXI Crimes of Kidnapping and Inducement, crimes provided for in Articles 297 through 301-2 and 305 from among Chapter XXXXII Crimes concerning Rape and Sexual Harassment, crimes provided for in Article 315 from among Chapter XXXIV Crimes Against Credit, Business and Auction, Articles 324-2 through 324-4, 324-5 (limited to attempted criminals provided for in Articles 324-2 through 324-4) from among Chapter XXXVII Crimes of Obstruction of Exercise of Rights, crimes provided for in Articles 329 through 331, 332 (limited to habitual criminals provided for in Articles 329 through 331), 333 through 341, 342 [limited to habitual criminals provided for in Articles 329 through 331, 333 (limited to habitual criminals provided for in Articles 329 through 331), 333 through 341)] from Chapter XXXVIII Crimes of Larceny and Robbery and crimes provided for in Article 350 from among Chapter XXXIX Crimes of Fraud and Intimidation;

2. Part II of the Military Criminal Act -- Chapter I Crimes of Rebellion, Chapter II Crimes of Benefitting the Enemy, Chapter III Crimes of Abuse of Command, Chapter IV Crimes of Surrender and Escape of Commanders, Chapter V Crimes of Desertion of Defensive Post, crimes under Article 42 from Chapter VII Crimes of Neglecting Military Duty, Chapter VIII Crimes of Mutiny, Chapter IX Crimes of Violence, Intimidation, Inflicting Bodily Injury and Homicide, Chapter XI Crimes concerning Military Supplies, crimes under Articles 78, 80 and 81 from Chapter XII Crimes of Disobedience to Order;

3. Crimes under the National Security Act;

4. Crimes under the Military Secret Protection Act;

5. Crimes under the Protection of Military Installations Act;

6. Crimes provided for in Articles 58 through 62 from among those under the Act on the Control of Narcotics, etc.;

7. Crimes provided for in Articles 4 and 5 from among those under the Punishment of Violences, etc. Act;

8. Crimes provided for in Article 70 and subparagraphs 1 through 3 of Article 71 from among those under the Control of Firearms, Swords, Explosives, etc. Act;

9. Crimes provided for in Articles 2 through 8 and 10 through 12 from among those under the Act on the Aggravated Punishment, etc. of Specific Crimes;

10. Crimes provided for in Articles 3 through 9 from among those under the Act on the Aggravated Punishment, etc. of Specific Economic Crimes; and

11. Crimes committed in violation of Acts requiring the aggravated punishment of crimes provided for in subparagraphs 1 and 2.

(2) The communication-restricting measures may be permitted when the target is any specific mail or telecommunications sent and received or transmitted and received by those falling under the conditions of paragraph (1) or any specific mail or telecommunications sent and received or transmitted and received by the applicable parties over a fixed period of time.

Article 6 (Procedures for Authorization of Communication-Restricting Measures for Criminal Investigation)

(1) Any prosecutor (including any public prosecutor; hereinafter the same shall apply) may ask a court (including a military court; hereinafter the same shall apply) to permit communication-restricting measures according to any suspect or any person under investigation when the requirements provided for in Article 5 (1) are met. <Amended by Act No. 6546, Dec. 29, 2001>

(2) A judicial police officer (including a military judicial police officer, hereinafter the same shall apply) may apply to a prosecutor for authorization of communication-restricting measures according to any suspect or any person under investigation when the requirements under Article 5 (1) are met, and then the public prosecutor may request the same from the court. <Amended by Act No. 6546, Dec. 29, 2001>

(3) The competent court in charge of the case of the communication-restricting measures for which a request is filed under paragraphs (1) and (2) shall be the district court or its branch court (including any ordinary military court) having jurisdiction over the address and seats of both of communication parties or one of the communication parties subject to the communication-restricting measures, the place where any crime is committed or the address and seats of persons who are accomplices of such communication parties. <Amended by Act No. 6546, Dec. 29, 2001>

(4) The request for communication-restricting measures under paragraphs (1) and (2) shall be made in writing (hereinafter referred to as "written application"), indicating the details of the request such as kinds, objectives, targets, scope, period of communication-restricting measures, the place where such communication-restricting measures are executed, how such communication-restricting measures are executed and grounds satisfying the conditions for the permission for communication-restricting measures under Article 5 (1), together with the materials establishing a prima facie case for the reasons of the application. In this case, when an application is filed for permission for the communication-restricting measures against any suspect or any person under investigation for the same crime or any permission for such purpose is granted, the applicant shall specify the objective of and the grounds for filing an application again for the communication-restricting measures. <Amended by Act No. 6546, Dec. 29, 2001>

(5) The court shall, when it deems the application justifiable, grant permission for the communication-restricting measures according to any suspect or any person under investigation

and then deliver a document attesting his granting such permission (hereinafter referred to as "written permission") to the applicant. <Amended by Act No. 6546, Dec. 29, 2001>

(6) The written permission referred to in paragraph (5) shall specify the kind, objective, object, scope, period, the place where the communication-restricting measures are executed and how the communication-restricting measures are executed. <Amended by Act No. 6546, Dec. 29, 2001>

(7) The period of communication-restricting measures shall not exceed 2 months and in the event that the objective of the communication-restricting measures is attained during the period, such communication-restricting measures shall be immediately discontinued: Provided, That if the requirements for permission under Article 5 (1) are still valid, a request for extending the period of communication-restricting measures pursuant to paragraphs (1) and (2) may be filed, within the limit of 2 months and such request shall be appended by material establishing a prima facie case. <Amended by Act No. 6546, Dec. 29, 2001>

(8) In cases where the court considers that the request is groundless, it shall dismiss it and notify the requester thereof.

Article 7 (Communication-Restricting Measures for National Security)

(1) The heads of the intelligence and investigative agencies (hereinafter referred to as "heads of intelligence and investigative agencies") may, only when the national security is expected to be put in danger and the collection of intelligence is required to prevent such danger, take communication-restricting measures according to the classifications falling under each of the following subparagraphs: <Amended by Act No. 6546, Dec. 29, 2001>

1. If either or both of the parties concerned with a communication are Korean nationals, permission therefor from a senior chief judge of the high court shall be obtained: Provided, That the same shall not apply to the military telecommunications (limited to a case where the telecommunications are used to carry out operations) provided for in Article 2 of the Military Telecommunications Act; and

2. Approval shall be obtained from the President in writing with respect to communications of countries hostile to the Republic of Korea, foreign agencies or groups and foreign nationals under suspicion of antinational activities, or members of groups within the Korean Peninsula in effect beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries, and in the event of the proviso of paragraph (1) 1.

(2) The period of communication-restricting measures under paragraph (1) shall not exceed 4 months, and in the event the objective of such communication-restricting measures is attained, the communication-restricting measures shall be immediately discontinued. If the requirements of paragraph (1) continue to be in existence, the period of the communication-restricting measures may be extended within the limit of 4 months with permission therefor from a senior chief judge of the high court or approval therefor from the President after filing an application for such permission or approval, accompanied by the material establishing a prima facie case: Provided, That the communication-restricting measures provided for in the proviso of paragraph (1) 1 may be extended without approval therefor from the President until military operations are completed in the event that the nation is in time of war or incident, or at war with enemy in the national emergency situation corresponding thereto. <Amended by Act No. 6546, Dec. 29, 2001>

(3) Article 6 (2), (4) through (6), and (8) shall apply to the permission referred to in paragraph (1) 1. In such cases, the term "judicial police officer (including military police officer; hereinafter the same shall apply)", "court", "Article 5 (1)", and "communication-restricting measures according to any suspect or any person under investigation" in Article 6 (2) and (5) shall be deemed the term "heads of intelligence and investigative agencies", "senior chief judge of the high court", "main sentence of Article 7 (1) 1", and "communication-restricting measures", respectively. <Amended by Act No. 6546, Dec. 29, 2001>

(4) Necessary matters such as procedures for a presidential approval referred to in paragraph (1) 2 shall be determined by the Presidential Decree.

Article 8 (Emergency Communication-Restricting Measures)

(1) In the event that an act of conspiracy exists that threatens the national security, the planning or execution of any serious crime or any organized crime, etc. is imminent that may cause directly the dangers of death or serious injuries, and the emergency grounds exist that make it impossible to go through the provisions of Article 6 or 7 (1) and (3), any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies may take the communication-restricting measures without permission therefor from the court against any person who meets the requirements provided for in Article 5 (1) or 7 (1) 1.

(2) Any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, immediately after the execution of the communication-restricting measures under paragraph (1) (hereinafter referred to as "emergency communication-restricting measures") commences, file an application for permission therefor with the court in accordance with Articles 6 and 7 (3), and get the emergency communication-restricting measures immediately discontinued if he fails to obtain the permission from the court within 36 hours from the time that he takes the emergency communication-restricting measures.

(3) If any judicial police officer takes the emergency communication-restricting measures, he shall be placed under command of any prosecutor in advance: Provided, That in case that if such emergency communication-restricting measures need to be taken urgently, leaving such judicial police officer impossible to be placed under command of such prosecutor, approval therefor shall be obtained from such prosecutor immediately after the execution of such emergency communication-restricting measures commences.

(4) In the event that any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, if he intends to take the emergency communication-restricting measures, take such measures according to the emergency censorship statement or the emergency wiretapping statement (hereinafter referred to as "emergency wiretapping statement. etc.") and keep the records of emergency communication-restricting measures at the institution to which he belongs.

(5) In the event that the execution of communication-restricting measures is completed in a short time, making it unnecessary to seek permission therefor from the court, the head of the competent District Public Prosecutor's Office (the head of the competent High Prosecutor's Office in case that any of the heads of intelligence and investigative agencies takes the emergency communication-restricting measures against any person who meets the requirements provided for in Article 7 (1) 1 in accordance with paragraph (1)) shall serve an emergency communication-restricting measures notice, prepared by any prosecutor, any judicial police officer or any of the heads of intelligence

and investigative agencies who takes the relevant communication-restricting measures, to the head of corresponding court: Provided, That in the event that any public prosecutor or any military judicial official takes the emergency communication-restricting measures against any person who meets the requirements provided for in Article 5 (1), a senior prosecutor of the competent Public Prosecutor's Office shall serve an emergency communication-restricting measures notice to the military judge corresponding to him of the ordinary military tribunal.

(6) The notice referred to in paragraph (5) shall contain the objective, subject, scope, period, the place of execution, method and the grounds for not filing a request for permission for the emergency communication-restricting measures, etc.

(7) The court or the military judge of the ordinary military tribunal shall, upon receiving the emergency communication-restricting measures notice served under paragraph (5), keep the records of emergency communication-restricting measures.

(8) In the event that an act of conspiracy exists that threatens the national security, the planning or execution of any serious crime or any organized crime, etc. is imminent that may cause directly the dangers of deaths or serious injuries, it is short of time for obtaining approval from the President for taking the emergency communication-restricting measures against any person who falls under Article 7 (1) 2 and it is judged that the national security may be put in danger unless the emergency communication-restricting measures are taken, any of the heads of intelligence and investigative agencies may take the emergency communication-restricting measures after obtaining approval therefor from the minister (including the Director General of the National Intelligence Agency) to whom he belongs.

(9) In the event that the emergency communication-restricting measures are taken in accordance with paragraph (8), approval therefor shall be obtained without any delay from the President in accordance with Article 7. If such approval fails to be obtained from the President within 36 hours from the time that an application therefor is filed, such emergency communication-restricting measures shall be immediately discontinued.

[This Article Wholly Amended by Act No. 6546, Dec. 29, 2001]

Article 9 (Execution of Communication-Restricting Measures)

(1) Communication-restricting measures under Articles 6 through 8 shall be executed by any public prosecutor, any judicial police officer or any of the heads of the intelligence and investigative agencies who has made such a request or application. In this case, the execution may be commissioned to or cooperation therewith may be sought from postal service organizations or other institutions concerned (hereinafter referred to as "communications institutions, etc."). <Amended by Act No. 6546, Dec. 29, 2001>

(2) Any person who intends to commission the execution of communication-restricting measures or ask for cooperation therewith, shall furnish any of the communications institutions, etc. with a written permission for the communication-restricting measures (referring to a written approval granted by the President in the case of Article 7 (1) 2; hereafter the same shall apply in Articles 16 (2) 1 and 17 (1) 1 and 3) or a copy of the cover of an emergency wiretapping statement, etc. Any person who is commissioned or asked for cooperation shall keep such written permission for the communication-restricting measures or such copy of the cover of an emergency wiretapping

statement for a period fixed by the Presidential Decree. <Amended by Act No. 6546, Dec. 29, 2001>

(3) Any person who executes the communication-restricting measures, is commissioned to execute such measures or asked for cooperation therewith shall keep records in which the objectives of the relevant communication-restricting measures, the execution of such measures, the date on which cooperation is made and the object of such cooperation are entered for a period fixed by the Presidential Decree. <Newly Inserted by Act No. 6546, Dec. 29, 2001>

(4) In the event that the telephone number, etc. of any person subject to the communication-restricting measures, which is entered in the written permission for communication-restricting measures or the emergency wiretapping statement, etc., is inconsistent with the fact, any of the communications institutions, etc. may refuse to execute the relevant communication-restricting measures and shall be prohibited from leaking secret numbers used for telecommunications in any case. <Newly Inserted by Act No. 6546, Dec. 29, 2001>

Article 9-2 (Notice on Execution of Communication-Restricting Measures)

(1) Any prosecutor shall, when he institutes a prosecution or takes a disposition not to institute any prosecution or indict in connection with a case involving the execution of the communication-restricting measures in accordance with Articles 6 (1) and 8 (1) (excluding any decision made to suspend any indictment), notify in writing a person subject to the mail censorship in the case of mail censorship and a subscriber to telecommunications who is subject to wiretapping in the case of wiretapping of the fact that the communication-restricting measures are executed, the institution that executes such measures and the period thereof, etc. within 30 days therefrom.

(2) Any judicial police officer shall, when he is notified by any prosecutor that the latter institutes a prosecution or takes a disposition not to institute a prosecution or indict in connection with a case involving the execution of the communication-restricting measures under Articles 6 (1) and 8 (1) (excluding any decision made to suspend any indictment) or he takes a disposition not to indict in connection with a case of a person under investigation, notify in writing a person subject to the mail censorship in the case of mail censorship and a subscriber to telecommunications who is subject to wiretapping in the case of wiretapping of the fact that the communication-restricting measures are executed, the institution that executes such measures and the period thereof, etc. within 30 days therefrom.

(3) Any of the heads of intelligence and investigative agencies shall notify in writing a person subject to the mail censorship in the case of mail censorship and a subscriber to telecommunications who is subject to wiretapping in the case of wiretapping of the fact that the communication-restricting measures are executed, the institution that executes such measures and the period thereof, etc. within 30 days from the date on which the communication-restricting measures taken in accordance with the main sentence of Article 7 (1) 1 and Article 8 (1) are completed.

(4) Notwithstanding the provisions of paragraphs (1) through (3), in the event that the grounds falling under each of the following subparagraphs accrue, the notice may be deferred until such grounds cease to exist:

1. When the notice of the communication-restricting measures is seriously feared to endanger the national security and disrupt the public safety and order; and

2. When the notice of the communication-restricting measures is feared to result in dangers to lives and bodies of people.

(5) Any prosecutor or any judicial police officer shall, when he intends to defer the notice in accordance with paragraph (4), obtain approval therefor from the head of the District Public Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with the District Prosecutor's Office: Provided, That in the event any public prosecutor or any military judicial police officer intends to defer the notice in accordance with paragraph (4), he shall obtain approval therefor from a senior prosecutor of the competent Public Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with such Public Prosecutor's Office.

(6) Any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, when the grounds referred to in each subparagraph of paragraph (4) cease to exist, serve the notice referred to in paragraphs (1) through (3) within 30 days from the date on which such grounds cease to exist.

[This Article Newly Inserted by Act No. 6546, Dec. 29, 2001]

Article 10 (Authorizing Agencies and Procedures for Tapping Equipment)

(1) Any person who intends to make, import, sell, distribute, possess, use or advertize any tapping equipment shall obtain an authorization of the Minister of Information and Communication: Provided, That this shall not apply in the cases of government agencies. <Amended by Act No. 5454, Dec. 13, 1997>

(2) Once the Minister of Information and Communication grants the authorization under paragraph (1), he shall secure an approval of the Prime Minister. <Amended by Act No. 5454, Dec. 13, 1997>

(3) In cases where the Minister of Information and Communication grants the authorization under paragraph (1), he shall enter the name of applicant for authorization, the date of authorization, kinds and quantity of authorized tapping equipment and other necessary matters in a register and keep it ready. <Amended by Act No. 5454, Dec. 13, 1997>

(4) Any person who makes, imports, sells, distributes, possesses or uses any tapping equipment with the authorization under paragraph (1) shall enter the date of authorization, kinds and quantity of authorized tapping equipment, location of installation and other necessary matters in a register and keep it ready: Provided, That the tapping equipment furnished those for performance of the duties of local bodies, that are fixtures of local government, shall be recorded in the register for fixtures of the applicable administrative body.

(5) Necessary matters relating to the authorization under paragraph (1) shall be determined by the Presidential Decree.

Article 10-2 (Report on Tapping Equipment Managed by State Organs)

(1) Any of state organs (excluding intelligence and investigative agencies) shall, when it introduces tapping equipment, report its dimensions and performances, including matters prescribed by the Presidential Decree, by half year, to the Minister of Information and Communication.

(2) Any of intelligence and investigative agencies shall, when it introduces tapping equipment, report its dimensions and performances, including matters prescribed by the Presidential Decree, by half year, to the Intelligence Committee of the National Assembly.

[This Article Newly Inserted by Act No. 6546, Dec. 29, 2001]

Article 11 (Obligation to Keep Secrets)

(1) Any public official or any former public official who has been engaged in the permission, execution, notice and preparation of various documents, etc. in connection with the communication-restricting measures shall be prohibited from disclosing or leaking matters concerning the communication-restricting measures he has learned while performing his duties.

(2) Any employee or any former employee of any communications institution shall be prohibited from disclosing or leaking matters concerning the communication-restricting measures.

(3) Any person other than those of paragraphs (1) and (2) shall be prohibited from disclosing or leaking what he has learned in connection with the communication-restricting measures except that his knowledge is used according to the provisions of this Act.

(4) Matters necessary to keep secret procedures for granting permission, whether to grant permission, the contents of permission, etc. for the communication-restricting measures by the court shall be prescribed by the rules of the Supreme Court.

[This Article Wholly Amended by Act No. 6546, Dec. 29, 2001]

Article 12 (Restriction on Use of Materials Acquired through Communication-Restricting Measures)

Mail or its contents and contents of any telecommunications acquired through execution of the communication-restricting measures referred to in Article 9 shall not be used except for the cases in each of the following subparagraphs:

1. A case where they are used to investigate, prosecute the crimes prescribed in Article 5 (1) that have become the objective of the communication-restricting measures or the crimes related hereto, or prevent such crimes;

2. A case where they are used in disciplinary proceedings for crimes under subparagraph 1;

3. A case where a party concerned in communication uses them in a claim for damages; and

4. A case where they are used under the provisions as prescribed in other Acts.

Article 13 (Procedures for Provision of Communication Confirmation Data)

(1) Any prosecutor or any judicial police officer may, when he deems it necessary to conduct any investigation or to execute any punishment, ask any operator of the telecommunications business (hereinafter referred to as "operator of telecommunications business") for the perusal or the provision of the communication confirmation data (hereinafter referred to as "provision of the communication confirmation data").

(2) Any of the heads of intelligence and investigative agencies may, when he deems it necessary to gather intelligence for the purpose of preventing any threat or danger to the national security,

ask any operator of the telecommunications business for the provision of the communication confirmation data.

(3) Any prosecutor or any judicial police officer shall, when he intends to ask for the provision of the communication confirmation data, obtain approval therefor from the head of the competent District Public Prosecutor's Office (referring to a senior prosecutor of the competent Public Prosecutor's Office in case that a public prosecutor or a military judicial police officer asks for the provision of the communication confirmation data): Provided, That, if the emergency grounds exist that make it impossible to obtain approval from the head of the District Public Prosecutor's Office, such approval shall be obtained immediately after asking for the provision of the communication confirmation data.

(4) Any request for the provision of the communication confirmation data under paragraphs (1) and (2) shall be filed in writing, specifying the grounds for filing such request, the relationship with the relevant subscriber and the scope of necessary data (hereinafter referred to as "written request for the provision of the communication confirmation data"): Provided, That when the emergency grounds exist that make it impossible to file a written request, a written request for the provision of the communication confirmation data shall be filed immediately after asking any operator of the telecommunications business for the provision of such communication confirmation data.

(5) Any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, when he is supplied with the communication confirmation data under paragraph (3) or (4), keep records in which necessary matters, including the fact of asking for the provision of the relevant communication confirmation data, etc. are entered and other relevant materials, including the written request for the provision of the communication conformation data, etc. at the institution to which he belongs.

(6) The head of the District Public Prosecutor's Office or a senior prosecutor of the Public Prosecutor's Office shall keep records with respect to granting approvals for requests for the provision of the communication confirmation data and other materials related thereto under paragraph (3).

(7) An operator of the telecommunications business shall, when he provides any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies with the communication confirmation data, make a report on the provision of the communication confirmation data twice a year to the Minister of Information and Communication, and keep records in which necessary matters, including the provisions of the communication confirmation data, are entered and other materials related to requests for the provision of the communication confirmation data, etc. for 7 years from the date on which each of such communication confirmation data is provided.

(8) The Minister of Information and Communication may check on the authenticity of reports made by operators of the telecommunications business under paragraph (7) and the management of related materials, including records, which need to be kept by them.

[This Article Newly Inserted by Act No. 6546, Dec. 29, 2001]

Article 13-2 (Provision of Communication Confirmation Data to Court)

Any court may, when it is deemed necessary for trial, ask any operator of the telecommunications business to provide it with the communication confirmation data under Article 294 of the Civil

Procedure Act and Article 272 of the Criminal Procedure Act. <Amended by Act No. 6626, Jan. 26, 2002>

[This Article Newly Inserted by Act No. 6546, Dec. 29, 2001]

Article 14 (Prohibition of Interference in Others' Conversation Secrets)

(1) No person shall record a conversation between others that is not open to the public or listen to it through the employment of electronic or mechanical devices.

(2) The provisions of Articles 4 through 8, the former part of Article 9 (1) and Articles 9, 9-2, 11 (1), (3) and (4) and 12 shall apply to recording or listening as referred to in paragraph (1). <Amended by Act No. 6546, Dec. 29, 2001>

Article 15 (Control of National Assembly)

(1) Any of the standing committees and any committee for inspection and investigation of state administration of the National Assembly may, when it is deemed necessary, ask the head of the Ministry of Court Administration to make a report on any specific communication-restricting measures, etc., the heads of agencies or institutions that have filed requests or applications for the communication-restricting measures or have executed such communication-restricting measures to make reports thereon and the Minister of Information and Communication to make a report detailing tapping equipment authorized and reports filed in connection of such tapping equipment, respectively.

(2) Any of the standing committees and any committee for inspection and investigation of state administration of the National Assembly may, by a decision, conduct on-the-spot inspection or other inspection on tapping equipment currently in possession of investigative agencies, telephone switchboard rooms and other places of agencies that have executed the tapping or institutions that have cooperated in tapping. In this case, any person participating in the on-the-spot inspection and other inspection shall be prohibited from leaking secrets he has learned therefrom without any justifiable grounds.

(3) The on-the-spot investigation or other investigation referred to in paragraph (2) shall not be conducted for the purpose of violating any person's privacy, intervening in any pending trial or the prosecution of a case under investigation.

(4) The head of any central administrative agency that has executed the communication-restricting measures, has been commissioned to execute such communication-restricting measures or has cooperated in executing the communication-restricting measures shall, upon receiving a request from any of the standing committees or any committee for inspection and investigation of state administration of the National Assembly, make a report on the communication-restricting measures related to Articles 5 through 10 to the National Assembly under the conditions as prescribed by the Presidential Decree: Provided, That any of the heads of intelligence and investigative agencies shall make such report to the Intelligence Committee of the National Assembly.

[This Article Wholly Amended by Act No. 6546, Dec. 29, 2001]

Article 16 (Penal Provisions)

(1) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 10 years or by suspension of qualification for not more than 5 years:

1. A person who has censored any mail, wiretapped any telecommunications or recorded and eavesdropped on any conversations between other individuals in violation of the provisions of Article 3; and

2. A person who has disclosed or leaked the substances of communications or conversations he has learned in a manner referred to in subparagraph 1.

(2) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 10 years:

1. A person who has commissioned the execution of communication-restricting measures or asked for cooperation in the execution of such communication-restricting measures without delivering a written permission for communication-restricting measures or a copy of the cover of an emergency wiretapping statement or any other persons who has executed commissioned communication-restricting measures or cooperated in the execution of such communication-restricting measures without receiving a written permission for communication-restricting measures or a copy of the cover of an emergency wiretapping statement in violation of the provisions of Article 9 (2); and

2. A person who has violated the provisons of Article 11 (1) (including a case where he is subject to the application of the provisions of Article 14 (2))

(3) Any person who has violated the provisions of Article 11 (2) shall be punished by imprisonment with prison labor for not more than 7 years.

(4) Any person who has violated the provisions of Article 11 (3) (including a case where he is subject to the application of the provisions of Article 14 (2)) shall be punished by imprisonment with prison labor for not more than 5 years.

[This Article Wholly Amended by Act No. 6546, Dec. 29, 2001]

Article 17 (Penal Provisions)

(1) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 5 years or by a fine not exceeding 30 million won:

1. A person who has failed to keep a cover copy of a written permission for communication-restricting measures or an emergency wiretapping statement, etc. in violation of the provisions of Article 9 (2);

2. A person who has failed to keep records in violation of the provisons of Article 9 (3) (including a case where he is subject to the application of the provisions of Article 14 (2));

3. A person who has failed to confirm a telephone number of any person subject to the communication-restricting measures, which is entered in the written permission for communication-restricting measures or the emergency wiretapping statement or leaked any password used for telecommunications in violation of the provisions of Article 9 (4);

4. A person who has manufactured, imported, sold, distributed, possessed or used tapping equipment, and advertised for such purposes without obtaining authorization thereof in violation of the provisons of Article 10 (1);

5. A person who has failed to make or keep authorization records of tapping equipment in violation of the provisions of Article 10 (3) and (4); and

6. A person who has been provided with the communication confirmation data or provided such data in violation of the provisions of Article 13 (4).

(2) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 3 years or by a fine not exceeding 10 million won:

1. A person who has failed to discontinue immediately the emergency communication-restricting measures in violation of the provisions of the latter part of Article 8 (2) or the latter part of Article 8 (9);

2. A person who has failed to serve notice with respect to the execution of the communication-restricting measures in violation of the provisions of Article 9-2 (including a case where he is subject to the application of the provisions of Article 14 (2)); and

3. A person who has failed to report the provisions of the communication confirmation data, etc. to the Minister of Information and Communication or to keep related materials in violation of the provisions of Article 13 (7).

[This Article Wholly Amended by Act No. 6546, Dec. 29, 2001]

Article 18 (Criminal Attempts)

Attempts of the crimes prescribed in Articles 16 and 17 shall be punished.

ADDENDA

(1) (Enforcement Date) This Act shall enter into force six months after the date of its promulgation.

(2) (Abolished Act) The Temporary Post Control Act shall hereby be abolished.

(3) (Transitional Measures) A person, possessing or having used any tapping equipment, who is subject to authorization at the time of enforcement of this Act, shall, with the authorization referred to in Article 10, prepare and keep a register within 3 months after the date of the enforcement of this Act; a person who violates it shall be subject to subparagraph 2 of Article 17.

ADDENDUM <Act No. 5454, Dec. 13, 1997>

This Act shall enter into force on January 1, 1998. (Proviso Omitted.)

ADDENDA <Act No. 5681, Jan. 21, 1999>

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation.

Articles 2 through 4

Omitted.

ADDENDA <Act No. 6146, Jan. 12, 2000>

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2000.

Articles 2 through 9

Omitted.

ADDENDA <Act No. 6305, Dec. 29, 2000>

Article 1 (Enforcement Date)

This Act shall enter into force on January 1, 2001.

Articles 2 through 8

Omitted.

ADDENDA Act No. 6346, Jan. 8, 2001>

(1) (Enforcement Date) This Act shall enter into force three months after the date of its promulgation. (Proviso Omitted.)

(2) Omitted.

ADDENDA <Act No. 6546, Dec. 29, 2001>

Article 1 (Enforcement Date)

This Act shall enter into force three months after the date of its promulgation.

Article 2 (Applicable Examples)

(1) The amended provisions of Articles 5 (1), 6 (1) through (7), 7 (1) through (3), 8, 9, 9-2 and 14 (2) shall apply, starting with the communication-restricting measures for which a request is filed for permission or approval (including a case where a judicial police officer files such request) or whose execution commences for the first time after the enforcement of this Act.

(2) The amended provisions of Articles 13 and 13-2 shall apply, starting with the communication confirmation data for which a request is filed for approval therefor or provision thereof for the first time after the enforcement of this Act.

Article 3 (Transitional Measures concerning Tapping Equipment of State Organs)

Any state organ that is in possession of tapping equipment at the time when this Act enters into force shall make a report thereon to the Minister of Information and Communication or serve a

notice thereon to the Intelligence Committee of the National Assembly in accordance with the amended provisions of Article 10-2 within 3 months after the enforcement of this Act.

Article 4 (Transitional Measures concerning Penal Provisions)

The application of the penal provisions to any act committed prior to the enforcement of this Act shall be governed by the previous provisions.

ADDENDA Act No. 6626, Jan. 26, 2002>

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2002.

Articles 2 through 7

Omitted.