

LEGISLATIVE HISTORY CHECKLIST

Compiled by the NJ State Law Library

LAWS of 1999

CHAPTER: 151

NJSA:2A:156A-2 et al
(Wiretapping)

BILL NO: A3014(Substituted for S1858)

SPONSOR(S):Malone and Holzapfel

DATE INTRODUCED:March 18, 1999

COMMITTEE:

ASSEMBLY: Judiciary

*SENATE:*Judiciary

AMENDED DURING PASSAGE:No

DATES OF PASSAGE:

*ASSEMBLY:*May 10, 1999

*SENATE:*June 21, 1999

DATE OF APPROVAL:June 30, 1999

THE FOLLOWING ARE ATTACHED IF AVAILABLE:

FINAL TEXT OF BILL: *YES*Original corrected copy
(Amendments during passage denoted by superscript numbers)

A3014

SPONSORS STATEMENT: *Yes* (Begins on page 10 of original bill)

COMMITTEE STATEMENT:

ASSEMBLY: *Yes*

SENATE: *Yes*

FLOOR AMENDMENT STATEMENTS: *No*

LEGISLATIVE FISCAL ESTIMATE: *Yes*

S1858

SPONSORS STATEMENT: *Yes (Begins on page 10 of original bill)*

Bill and Sponsor Statement identical to A3014

COMMITTEE STATEMENT:

ASSEMBLY:*No*

SENATE:*Yes*

Identical to Senate Statement for A3014

FLOOR AMENDMENT STATEMENTS: *No*

LEGISLATIVE FISCAL ESTIMATE: *No*

GOVERNOR'S ACTIONS

VETO MESSAGE: *No*

GOVERNOR'S PRESS RELEASE ON SIGNING: *Yes*

THE FOLLOWING WERE PRINTED:

To check for circulating copies contact New Jersey State Government Publications at the State Library (609) 278-2640 ext. 102 or refdesk@njstatelib.org

REPORTS: *No*

HEARINGS: *No*

NEWSPAPER ARTICLES: *No*

P.L. 1999, CHAPTER 151, *approved June 30, 1999*
Assembly, No. 3014 (*Corrected Copy*)

1 **AN ACT** concerning wiretapping and electronic surveillance and
2 amending P.L.1968, c.409 and P.L.1993, c.29.

3

4 **BE IT ENACTED** *by the Senate and General Assembly of the State*
5 *of New Jersey:*

6

7 1. Section 28 of P.L.1968, c.409 is amended to read as follows:

8 28. This act shall take effect January 1, 1969 [and remain in effect
9 until July 1, 1999].

10 (cf: P.L.1994, c.55, s.1)

11

12 2. Section 2 of P.L.1968, c.409 (C.2A:156A-2) is amended to read
13 as follows:

14 2. As used in this act:

15 a. "Wire communication" means any aural transfer made in whole
16 or in part through the use of facilities for the transmission of
17 communications by the aid of wire, cable or other like connection
18 between the point of origin and the point of reception, including the
19 use of such connection in a switching station, furnished or operated by
20 any person engaged in providing or operating such facilities for the
21 transmission of intrastate, interstate or foreign communication. "Wire
22 communication" includes any electronic storage of such
23 communication, and the radio portion of a cordless telephone
24 communication that is transmitted between the cordless telephone
25 handset and the base unit;

26 b. "Oral communication" means any oral communication uttered
27 by a person exhibiting an expectation that such communication is not
28 subject to interception under circumstances justifying such
29 expectation, but does not include any electronic communication;

30 c. "Intercept" means the aural or other acquisition of the contents
31 of any wire, electronic or oral communication through the use of any
32 electronic, mechanical, or other device;

33 d. "Electronic, mechanical or other device" means any device or
34 apparatus, including an induction coil, that can be used to intercept a
35 wire, electronic or oral communication other than:

36 (1) Any telephone or telegraph instrument, equipment or facility,
37 or any component thereof, furnished to the subscriber or user by a
38 provider of wire or electronic communication service in the ordinary
39 course of its business and being used by the subscriber or user in the
40 ordinary course of its business; or furnished by such subscriber or user
41 for connection to the facilities of such service and used in the ordinary

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

1 course of its business; or being used by a provider of wire or electronic
2 communication service in the ordinary course of its business, or by an
3 investigative or law enforcement officer in the ordinary course of his
4 duties; or

5 (2) A hearing aid or similar device being used to correct subnormal
6 hearing to not better than normal;

7 e. "Person" means that term as defined in R.S.1:1-2 and includes
8 any officer or employee of the State or of a political subdivision
9 thereof;

10 f. "Investigative or law enforcement officer" means any officer of
11 the State of New Jersey or of a political subdivision thereof who is
12 empowered by law to conduct investigations of, or to make arrests for,
13 any offense enumerated in section 8 of P.L.1968, c.409
14 (C.2A:156A-8) and any attorney authorized by law to prosecute or
15 participate in the prosecution of any such offense;

16 g. "Contents," when used with respect to any wire, electronic or
17 oral communication, includes any information concerning the identity
18 of the parties to such communication or the existence, substance,
19 purport, or meaning of that communication, except that for purposes
20 of sections 22, 23, 24 and 26 of P.L.1993, c.29 (C.2A:156A-28,
21 C.2A:156A-29, C.2A:156A-30, and C.2A:156A-32) contents, when
22 used with respect to any wire, electronic, or oral communication
23 means any information concerning the substance, purport or meaning
24 of that communication;

25 h. "Court of competent jurisdiction" means the Superior Court;

26 i. "Judge," when referring to a judge authorized to receive
27 applications for, and to enter, orders authorizing interceptions of wire,
28 electronic or oral communications, means one of the several judges of
29 the Superior Court to be designated from time to time by the Chief
30 Justice of the Supreme Court to receive applications for, and to enter,
31 orders authorizing interceptions of wire, electronic or oral
32 communications pursuant to this act;

33 j. "Communication common carrier" means any person engaged as
34 a common carrier for hire, in intrastate, interstate or foreign
35 communication by wire or radio or in intrastate, interstate or foreign
36 radio transmission of energy; but a person engaged in radio
37 broadcasting shall not, while so engaged, be deemed a common
38 carrier;

39 k. "Aggrieved person" means a person who was a party to any
40 intercepted wire, electronic or oral communication or a person against
41 whom the interception was directed;

42 l. "In-progress trace" means the determination of the origin of a
43 telephonic communication to a known telephone during the
44 communication;

45 m. "Electronic communication" means any transfer of signs,
46 signals, writing, images, sounds, data, or intelligence of any nature

1 transmitted in whole or in part by a wire, radio, electromagnetic,
2 photoelectric or photo-optical system that affects interstate, intrastate
3 or foreign commerce, but does not include:

4 (1) Any wire or oral communication;
5 (2) Any communication made through a tone-only paging device;
6 or

7 (3) Any communication from a tracking device;

8 n. "User" means any person or entity who:

9 (1) Uses an electronic communication service; and

10 (2) Is duly authorized by the provider of such service to engage in
11 such use;

12 o. "Electronic communication system" means any wire, radio,
13 electromagnetic, photo-optical or photoelectronic facilities for the
14 transmission of electronic communications, and any computer facilities
15 or related electronic equipment for the electronic storage of such
16 communications;

17 p. "Electronic communication service" means any service which
18 provides to the users thereof the ability to send or receive wire or
19 electronic communications;

20 q. "Electronic storage" means:

21 (1) Any temporary, intermediate storage of a wire or electronic
22 communication incidental to the electronic transmission thereof; and

23 (2) Any storage of such communication by an electronic
24 communication service for purpose of backup protection of the
25 communication;

26 r. "Readily accessible to the general public" means, with respect
27 to a radio communication, that such communication is not:

28 (1) Scrambled or encrypted;

29 (2) Transmitted using modulation techniques whose essential
30 parameters have been withheld from the public with the intention of
31 preserving the privacy of such communication;

32 (3) Carried on a subcarrier or other signal subsidiary to a radio
33 transmission;

34 (4) Transmitted over a communication system provided by a
35 common carrier, unless the communication is a tone-only paging
36 system communication; or

37 (5) Transmitted on frequencies allocated under part 25, subpart D,
38 E, or F of part 74, or part 94 of the Rules of the Federal
39 Communications Commission, unless, in the case of a communication
40 transmitted on a frequency allocated under part 74 that is not
41 exclusively allocated to broadcast auxiliary services, the
42 communication is a two-way voice communication by radio;

43 s. "Remote computing service" means the provision to the public
44 of computer storage or processing services by means of an electronic
45 communication system;

46 t. "Aural transfer" means a transfer containing the human voice at

1 any point between and including the point of origin and the point of
2 reception;

3 u. "Tracking device" means an electronic or mechanical device
4 which permits the tracking of the movement of a person or device;

5 v. "Point of interception" means the site at which the investigative
6 or law enforcement officer is located at the time the interception is
7 made.

8 (cf: P.L.1993,c.29,s.1)

9

10 3. Section 4 of P.L.1968, c.409 (C.2A:156A-4) is amended to read
11 as follows:

12 4. It shall not be unlawful under this act for:

13 a. An operator of a switchboard, or an officer, agent or employee
14 of a provider of wire or electronic communication service, whose
15 facilities are used in the transmission of a wire or electronic
16 communication, to intercept, disclose or use that communication in the
17 normal course of his employment while engaged in any activity which
18 is a necessary incident to the rendition of his service or to the
19 protection of the rights or property of the provider of that service. No
20 provider of wire or electronic communication service shall utilize
21 service observing or random monitoring except for mechanical or
22 service quality control checks;

23 b. Any investigative or law enforcement officer to intercept a wire,
24 electronic or oral communication, where such officer is a party to the
25 communication or where another officer who is a party to the
26 communication requests or requires him to make such interception;

27 c. Any person acting at the direction of an investigative or law
28 enforcement officer to intercept a wire, electronic or oral
29 communication, where such person is a party to the communication or
30 one of the parties to the communication has given prior consent to
31 such interception; provided, however, that no such interception shall
32 be made [~~unless the~~] without the prior approval of the Attorney
33 General or his designee or a county prosecutor [~~within his authority~~
34 determines that there exists a reasonable suspicion that evidence of
35 criminal conduct will be derived from such interception] or his
36 designee;

37 d. A person not acting under color of law to intercept a wire,
38 electronic or oral communication, where such person is a party to the
39 communication or one of the parties to the communication has given
40 prior consent to such interception unless such communication is
41 intercepted or used for the purpose of committing any criminal or
42 tortious act in violation of the Constitution or laws of the United
43 States or of this State or for the purpose of committing any other
44 injurious act. The fact that such person is the subscriber to a
45 particular telephone does not constitute consent effective to authorize
46 interception of communications among parties not including such

1 person on that telephone. Any person who unlawfully intercepts or
2 uses such communication as provided in this paragraph shall be subject
3 to the civil liability established in section 24 of P.L.1968, c.409
4 (C.2A:156A-24), in addition to any other criminal or civil liability
5 imposed by law;

6 e. Any person to intercept or access an electronic communication
7 made through an electronic communication system that is configured
8 so that such electronic communication is readily accessible to the
9 general public;

10 f. Any person to intercept any radio communication which is
11 transmitted:

12 (1) by any station for the use of the general public, or that relates
13 to ships, aircraft, vehicles, or persons in distress;

14 (2) by any governmental, law enforcement, civil defense, private
15 land mobile, or public safety communication system, including police
16 and fire, readily accessible to the general public;

17 (3) by a station operating on an authorized frequency within the
18 bands allocated to the amateur, citizens band, or general mobile radio
19 services; or

20 (4) by any marine or aeronautical communications system;

21 g. Any person to engage in any conduct which:

22 (1) is prohibited by section 633 of the Communications Act of
23 1934; or

24 (2) is excepted from the application of section 705(a) of the
25 Communications Act of 1934 by section 705(b) of that Act;

26 h. Any person to intercept any wire or electronic communication
27 the transmission of which is causing harmful interference to any
28 lawfully operating station or consumer electronic equipment, to the
29 extent necessary to identify the source of such interference; or for
30 other users of the same frequency to intercept any radio
31 communication made through a system that utilizes frequencies
32 monitored by individuals engaged in the provision or the use of such
33 system, if such communication is not scrambled or encrypted; or

34 i. A provider of [wire or] electronic communication service to
35 record the fact that a wire or electronic communication was initiated
36 or completed in order to protect such provider, another provider
37 furnishing service toward the completion of the wire or electronic
38 communication, or a user of that service, from fraudulent, unlawful or
39 abusive use of such service.

40 (cf: P.L.1993,c.29,s.3)

41

42 4. Section 8 of P.L.1968, c.409 (C.2A:156A-8) is amended to read
43 as follows:

44 8. The Attorney General, county prosecutor or a person
45 designated to act for such an official and to perform his duties in and
46 during his actual absence or disability, may authorize, in writing, an ex

1 parte application to a judge designated to receive the same for an
2 order authorizing the interception of a wire, or electronic or oral
3 communication by the investigative or law enforcement officers or
4 agency having responsibility for an investigation when such
5 interception may provide evidence of the commission of the offense of
6 murder, kidnapping, gambling, robbery, bribery, a violation of
7 paragraph (1) or (2) of subsection b. of N.J.S.2C:12-1, a violation of
8 section 3 of P.L. 1997, c.353 (C.2C:21-4.3), a violation of
9 N.J.S.2C:21-19 punishable by imprisonment for more than one year,
10 a violation of P.L.1994, c.121 (C.2C:21-23 et seq.), terroristic
11 threats, violations of N.J.S.2C:35-3, N.J.S.2C:35-4 and
12 N.J.S.2C:35-5, violations of sections 112 through 116, inclusive, of
13 the "Casino Control Act," P.L.1977, c.110 (C.5:12-112 through
14 5:12-116), arson, burglary, theft and related offenses punishable by
15 imprisonment for more than one year, endangering the welfare of a
16 child pursuant to N.J.S.2C:24-4, escape, forgery and fraudulent
17 practices punishable by imprisonment for more than one year,
18 alteration of motor vehicle identification numbers, unlawful
19 manufacture, purchase, use, or transfer of firearms, unlawful
20 possession or use of destructive devices or explosives, racketeering or
21 a violation of subsection g. of N.J.S.2C:5-2, leader of organized crime,
22 organized criminal activity directed toward the unlawful
23 transportation, storage, disposal, discharge, release, abandonment or
24 disposition of any harmful, hazardous, toxic, destructive, or polluting
25 substance, or any conspiracy to commit any of the foregoing offenses
26 or which may provide evidence aiding in the apprehension of the
27 perpetrator or perpetrators of any of the foregoing offenses.
28 (cf: P.L.1999, c.25, s.1)

29

30 5. Section 12 of P.L.1968, c.409 (C.2A:156A-12) is amended to
31 read as follows:

32 12. Each order authorizing the interception of any wire, electronic
33 or oral communication shall state:

34 a. The judge is authorized to issue the order;

35 b. The identity of, or a particular description of, the person, if
36 known, whose communications are to be intercepted;

37 c. The character and location of the particular communication
38 facilities as to which, or the particular place of the communication as
39 to which, authority to intercept is granted, or, in the case of an
40 application meeting the requirements of subsection g. of section 9 of
41 P.L.1968, c.409 (C.2A:156A-9) that specification is not practical or
42 that the purpose to thwart interception by changing facilities has been
43 shown;

44 d. A particular description of the type of the communication to be
45 intercepted and a statement of the particular offense to which it
46 relates;

1 e. The identity of the investigative or law enforcement officers or
2 agency to whom the authority to intercept a wire, electronic or oral
3 communication is given and the identity of whoever authorized the
4 application; and

5 f. The period of time during which such interception is authorized,
6 including a statement as to whether or not the interception shall
7 automatically terminate when the described communication has been
8 first obtained.

9 No order entered under this section shall authorize the interception
10 of any wire, electronic or oral communication for a period of time in
11 excess of that necessary under the circumstances. Every order entered
12 under this section shall require that such interception begin and
13 terminate as soon as practicable and be conducted in such a manner as
14 to minimize or eliminate the interception of such communications not
15 otherwise subject to interception under this act by making reasonable
16 efforts, whenever possible, to reduce the hours of interception
17 authorized by said order. In the event the intercepted communication
18 is in a language other than English, or is in a code, and an interpreter
19 or expert in that language or code is not reasonably available during
20 the interception period or a portion of the interception period,
21 minimization shall be accomplished as soon as practicable after the
22 interception. Except as provided below in subsection g. of this
23 section, no order entered under this section shall authorize the
24 interception of wire, electronic or oral communications for any period
25 exceeding 20 days. Extensions or renewals of such an order may be
26 granted for two additional periods of not more than 10 days. No
27 extension or renewal shall be granted unless an application for it is
28 made in accordance with this section, and the court makes the findings
29 required by sections 10 and 11 of P.L.1968, c.409 (C.2A:156A-10 and
30 2A:156A-11) and by this section.

31 g. Orders entered under this section to provide evidence of
32 racketeering in violation of N.J.S.2C:41-2, leader of organized crime
33 in violation of subsection g. of N.J.S.2C:5-2, or leader of narcotics
34 trafficking network in violation of N.J.S.2C:35-3, may authorize the
35 interception of wire, electronic or oral communications for a period
36 not to exceed 30 days and extensions or renewals of any order may be
37 granted for additional periods of not more than 30 days, without
38 limitation on the number of extension or renewal orders; provided,
39 however, that orders authorized pursuant to this subsection shall not
40 exceed six months.

41 h. Whenever an order authorizing an interception is entered, the
42 order may require reports to be made to the judge who issued the
43 order showing what progress has been made toward achievement of
44 the authorized objective and the need for continued interception. Such
45 reports shall be made at such intervals as the court may require.

46 An order authorizing the interception of a wire, electronic or oral

1 communication shall, upon request of the applicant, direct that a
2 provider of [wire or]electronic communication service shall furnish
3 the applicant forthwith all information, facilities and technical
4 assistance necessary to accomplish the interception unobtrusively and
5 with a minimum of interference with the services that such provider is
6 affording the person whose communications are to be intercepted.

7 The obligation of a provider of [wire or] electronic communication
8 service under such an order shall include but is not limited to
9 conducting an in-progress trace during an interception and shall also
10 include the provision of technical assistance and equipment and
11 utilization of any technological features which are available to the
12 provider of [wire or] electronic communication service. The
13 obligation of the provider of [wire or] electronic communication
14 service to conduct an in-progress trace and provide other technical
15 assistance may arise pursuant to court order based upon probable
16 cause, under circumstances not involving an interception pursuant to
17 this act. Any provider of [wire or] electronic communication service
18 furnishing such facilities or assistance shall be compensated therefor
19 by the applicant at the prevailing rates. Said provider shall be immune
20 from civil liability for any assistance rendered to the applicant pursuant
21 to this section.

22 An order authorizing the interception of a wire, electronic or oral
23 communication may be executed at any point of interception within
24 the jurisdiction of an investigative or law enforcement officer
25 executing the order.

26 (cf: P.L.1993,c.29,s.11)

27

28 6. Section 23 of P.L.1993, c.29 (C.2A:156A-29) is amended to
29 read as follows:

30 23. Requirements for access.

31 a. A law enforcement agency, but no other governmental entity,
32 may require the disclosure by a provider of [wire or] electronic
33 communication service or remote computing service of the contents of
34 an electronic communication without notice to the subscriber or the
35 customer if the law enforcement agency obtains a warrant.

36 b. Except as provided in subsection c. of this section, a provider
37 of electronic communication service or remote computing service may
38 disclose a record or other information pertaining to a subscriber or
39 customer of the service to any person other than a governmental
40 entity. This subsection shall not apply to the contents covered by
41 subsection a. of this section.

42 c. A provider of [wire or] electronic communication service or
43 remote computing service shall disclose a record or other information
44 pertaining to a subscriber or customer of the service, other than
45 contents covered by [subsection] subsections a. and f. of this section,
46 to a law enforcement agency under the following circumstances:

- 1 (1) the law enforcement agency has obtained a warrant; [or]
2 (2) the law enforcement agency has obtained the consent of the
3 subscriber or customer to the disclosure; or
4 (3) the law enforcement agency has obtained a court order for such
5 disclosure under subsection e. of this section.

6 A law enforcement agency receiving records or information
7 pursuant to this subsection is not required to provide notice to the
8 customer or subscriber.

9 d. Notwithstanding any other provision of law to the contrary, no
10 service provider, its officers, employees, agents or other specified
11 persons shall be liable in any civil action for damages as a result of
12 providing information, facilities or assistance in accordance with the
13 terms of a court order or warrant under this section.

14 e. A court order for disclosure under subsections b. or c. may be
15 issued by a judge of competent jurisdiction and shall issue only if the
16 law enforcement agency offers specific and articulable facts showing
17 that there are reasonable grounds to believe that the record or other
18 information pertaining to a subscriber or customer of an electronic
19 communication service or remote computing service is relevant and
20 material to an ongoing criminal investigation. A judge who has issued
21 an order pursuant to this section, on a motion made promptly by the
22 service provider, may quash or modify such order, if the information
23 or records requested are unusually voluminous in nature or compliance
24 with such order otherwise would cause an undue burden on such
25 provider.

26 f. A provider of electronic communication service or remote
27 computing service shall disclose to a law enforcement agency the
28 name, address, telephone number or other subscriber number or
29 identity, and length of service provided to a subscriber or customer of
30 such service and the types of services the subscriber or customer
31 utilized, when the law enforcement entity obtains a grand jury or trial
32 subpoena.

33 g. Upon the request of a law enforcement agency, a provider of
34 wire or electronic communication service or a remote computing
35 service shall take all necessary steps to preserve, for a period of 90
36 days, records and other evidence in its possession pending the issuance
37 of a warrant. The preservation period shall be extended for an
38 additional 90 days upon the request of the law enforcement agency.

39 (cf: P.L.1994,c.55,s.2)

40

41 7. This act shall take effect immediately .

42

43

STATEMENT

44

45 This bill amends the "New Jersey Wiretapping and Electronic
46 Surveillance Act" in order to address the problems facing law

1 enforcement agencies with regard to new technologies and to clarify
2 the procedures pertaining to the disclosure of information by the
3 providers to the law enforcement agencies.

4 The bill amends that provision of the act concerning ex-parte
5 orders. The act authorizes the Attorney General or a county
6 prosecutor to seek an ex-parte order allowing the interception of a
7 wire, electronic or oral communication for an investigation when the
8 investigation may provide evidence of the commission of an offense,
9 including but not limited to: murder, kidnapping, gambling, robbery
10 bribery, money laundering, terroristic threats, certain drug offenses,
11 violations of the "Casino Control Act," endangering the welfare of a
12 child or racketeering. This bill would expand the list to include health
13 care claims fraud, N.J.S.A. 2C:21-4.3. This bill would also clarify that
14 the list of enumerated offenses includes fraudulent practices punishable
15 by a term of imprisonment of more than one year.

16 Although the act requires that any order to intercept begin and
17 terminate as soon as practicable and that the interception be conducted
18 in a manner which minimizes the interception of communication not
19 otherwise subject to the order, there are instances when a law
20 enforcement agency may be faced with the situation where the
21 intercepted communication is in a language other than English or is
22 in code. If this is the case and an interpreter or expert is not available
23 during the interception period, the bill requires that the minimized
24 interception must be accomplished as soon as practicable. These
25 requirements are consistent with federal law. In addition, the bill
26 provides that an order authorizing interception may be executed at any
27 point of interception within the jurisdiction of an investigative or law
28 enforcement officer executing the order. The bill defines "point of
29 interception" as the site at which the investigative or law enforcement
30 officer is located at the time the interception is made.

31 This bill would also amend that provision of the act concerning the
32 disclosure by a provider of electronic communication service or
33 remote computing service to a law enforcement agency of the
34 contents of a subscriber's or customer's communication or the
35 disclosure of a subscriber's or customer's information. The act
36 provides that a law enforcement officer who has obtained a warrant
37 may require a provider to disclose the contents of a communication
38 without providing notice to the subscriber or the customer. The act
39 also provides that a provider shall disclose a record or other
40 information pertaining to a subscriber or customer of the service, other
41 than the contents of the communication, provided the law
42 enforcement agency obtains a warrant or consent from the subscriber
43 or customer. This bill would amend this section of the act to
44 authorize the provider to disclose the information if the law
45 enforcement agency obtained an order for disclosure. An order for
46 disclosure may be issued by a judge only if the law enforcement

1 agency offers specific and articulable facts showing that there are
2 reasonable grounds to believe that the record or other information
3 pertaining to a subscriber or customer of a service is relevant and
4 material to an ongoing criminal investigation. The judge who has
5 issued such an order may quash or modify the order, on a motion by
6 the service provider, if the information or records requested are
7 unusually voluminous in nature or compliance with such an order
8 would otherwise cause an undue burden on the provider. This bill also
9 requires a provider to disclose to a law enforcement agency, when the
10 law enforcement entity obtains a grand jury or trial subpoena, such
11 information as: the subscriber's name, address, telephone number or
12 other number or identity, the length of service provided and the types
13 of services utilized by the subscriber. In addition, the bill provides
14 that, upon the request of a law enforcement agency, a provider shall
15 take all necessary steps to preserve, for a period of 90 days, records
16 and other evidence in its possession pending the issuance of a warrant.
17 The preservation period shall be extended for an additional 90 days
18 upon the request of the law enforcement agency.

19 The bill also implements a technical change for consistency with the
20 federal law by deleting several references to wire communication
21 service. Wire communication service is included within the definition
22 of electronic communication service. Hence, these changes are not
23 intended to and do not make any substantive changes to the act.

24 In addition, this bill would eliminate the sunset provision, making
25 the act permanent. Currently, the act has a sunset provision which
26 requires the Legislature to re-authorize the act every several years.
27 The act is due to expire on July 1, 1999.

28

29

30

31

32 Amends the "New Jersey Wiretapping and Electronic Surveillance
33 Act."

ASSEMBLY, No. 3014

STATE OF NEW JERSEY 208th LEGISLATURE

INTRODUCED MARCH 18, 1999

Sponsored by:

Assemblyman JOSEPH R. MALONE, III
District 30 (Burlington, Monmouth and Ocean)
Assemblyman JAMES W. HOLZAPFEL
District 10 (Monmouth and Ocean)

Co-Sponsored by:

Assemblyman Cottrell

SYNOPSIS

Amends the "New Jersey Wiretapping and Electronic Surveillance Act."

CURRENT VERSION OF TEXT

As introduced.



1 AN ACT concerning wiretapping and electronic surveillance and
2 amending P.L.1968, c.409 and P.L.1993, c.29.

3

4 **BE IT ENACTED** by the Senate and General Assembly of the State
5 of New Jersey:

6

7 1. Section 28 of P.L.1968, c.409 is amended to read as follows:

8 28. This act shall take effect January 1, 1969 **[and remain in effect**
9 **until July 1, 1999]**.

10 (cf: P.L.1994, c.55, s.1)

11

12 2. Section 2 of P.L.1968, c.409 (C.2A:156A-2) is amended to read
13 as follows:

14 2. As used in this act:

15 a. "Wire communication" means any aural transfer made in whole
16 or in part through the use of facilities for the transmission of
17 communications by the aid of wire, cable or other like connection
18 between the point of origin and the point of reception, including the
19 use of such connection in a switching station, furnished or operated by
20 any person engaged in providing or operating such facilities for the
21 transmission of intrastate, interstate or foreign communication. "Wire
22 communication" includes any electronic storage of such
23 communication, and the radio portion of a cordless telephone
24 communication that is transmitted between the cordless telephone
25 handset and the base unit;

26 b. "Oral communication" means any oral communication uttered
27 by a person exhibiting an expectation that such communication is not
28 subject to interception under circumstances justifying such
29 expectation, but does not include any electronic communication;

30 c. "Intercept" means the aural or other acquisition of the contents
31 of any wire, electronic or oral communication through the use of any
32 electronic, mechanical, or other device;

33 d. "Electronic, mechanical or other device" means any device or
34 apparatus, including an induction coil, that can be used to intercept a
35 wire, electronic or oral communication other than:

36 (1) Any telephone or telegraph instrument, equipment or facility,
37 or any component thereof, furnished to the subscriber or user by a
38 provider of wire or electronic communication service in the ordinary
39 course of its business and being used by the subscriber or user in the
40 ordinary course of its business; or furnished by such subscriber or user
41 for connection to the facilities of such service and used in the ordinary
42 course of its business; or being used by a provider of wire or electronic
43 communication service in the ordinary course of its business, or by an

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

- 1 investigative or law enforcement officer in the ordinary course of his
2 duties; or
- 3 (2) A hearing aid or similar device being used to correct subnormal
4 hearing to not better than normal;
- 5 e. "Person" means that term as defined in R.S.1:1-2 and includes
6 any officer or employee of the State or of a political subdivision
7 thereof;
- 8 f. "Investigative or law enforcement officer" means any officer of
9 the State of New Jersey or of a political subdivision thereof who is
10 empowered by law to conduct investigations of, or to make arrests for,
11 any offense enumerated in section 8 of P.L.1968, c.409
12 (C.2A:156A-8) and any attorney authorized by law to prosecute or
13 participate in the prosecution of any such offense;
- 14 g. "Contents," when used with respect to any wire, electronic or
15 oral communication, includes any information concerning the identity
16 of the parties to such communication or the existence, substance,
17 purport, or meaning of that communication, except that for purposes
18 of sections 22, 23, 24 and 26 of P.L.1993, c.29 (C.2A:156A-28,
19 C.2A:156A-29, C.2A:156A-30, and C.2A:156A-32) contents, when
20 used with respect to any wire, electronic, or oral communication
21 means any information concerning the substance, purport or meaning
22 of that communication;
- 23 h. "Court of competent jurisdiction" means the Superior Court;
- 24 i. "Judge," when referring to a judge authorized to receive
25 applications for, and to enter, orders authorizing interceptions of wire,
26 electronic or oral communications, means one of the several judges of
27 the Superior Court to be designated from time to time by the Chief
28 Justice of the Supreme Court to receive applications for, and to enter,
29 orders authorizing interceptions of wire, electronic or oral
30 communications pursuant to this act;
- 31 j. "Communication common carrier" means any person engaged as
32 a common carrier for hire, in intrastate, interstate or foreign
33 communication by wire or radio or in intrastate, interstate or foreign
34 radio transmission of energy; but a person engaged in radio
35 broadcasting shall not, while so engaged, be deemed a common
36 carrier;
- 37 k. "Aggrieved person" means a person who was a party to any
38 intercepted wire, electronic or oral communication or a person against
39 whom the interception was directed;
- 40 l. "In-progress trace" means the determination of the origin of a
41 telephonic communication to a known telephone during the
42 communication;
- 43 m. "Electronic communication" means any transfer of signs,
44 signals, writing, images, sounds, data, or intelligence of any nature
45 transmitted in whole or in part by a wire, radio, electromagnetic,
46 photoelectric or photo-optical system that affects interstate, intrastate

- 1 or foreign commerce, but does not include:
- 2 (1) Any wire or oral communication;
- 3 (2) Any communication made through a tone-only paging device;
- 4 or
- 5 (3) Any communication from a tracking device;
- 6 n. "User" means any person or entity who:
- 7 (1) Uses an electronic communication service; and
- 8 (2) Is duly authorized by the provider of such service to engage in
- 9 such use;
- 10 o. "Electronic communication system" means any wire, radio,
- 11 electromagnetic, photo-optical or photoelectronic facilities for the
- 12 transmission of electronic communications, and any computer facilities
- 13 or related electronic equipment for the electronic storage of such
- 14 communications;
- 15 p. "Electronic communication service" means any service which
- 16 provides to the users thereof the ability to send or receive wire or
- 17 electronic communications;
- 18 q. "Electronic storage" means:
- 19 (1) Any temporary, intermediate storage of a wire or electronic
- 20 communication incidental to the electronic transmission thereof; and
- 21 (2) Any storage of such communication by an electronic
- 22 communication service for purpose of backup protection of the
- 23 communication;
- 24 r. "Readily accessible to the general public" means, with respect
- 25 to a radio communication, that such communication is not:
- 26 (1) Scrambled or encrypted;
- 27 (2) Transmitted using modulation techniques whose essential
- 28 parameters have been withheld from the public with the intention of
- 29 preserving the privacy of such communication;
- 30 (3) Carried on a subcarrier or other signal subsidiary to a radio
- 31 transmission;
- 32 (4) Transmitted over a communication system provided by a
- 33 common carrier, unless the communication is a tone-only paging
- 34 system communication; or
- 35 (5) Transmitted on frequencies allocated under part 25, subpart D,
- 36 E, or F of part 74, or part 94 of the Rules of the Federal
- 37 Communications Commission, unless, in the case of a communication
- 38 transmitted on a frequency allocated under part 74 that is not
- 39 exclusively allocated to broadcast auxiliary services, the
- 40 communication is a two-way voice communication by radio;
- 41 s. "Remote computing service" means the provision to the public
- 42 of computer storage or processing services by means of an electronic
- 43 communication system;
- 44 t. "Aural transfer" means a transfer containing the human voice at
- 45 any point between and including the point of origin and the point of
- 46 reception;

1 u. "Tracking device" means an electronic or mechanical device
2 which permits the tracking of the movement of a person or device;

3 v. "Point of interception" means the site at which the investigative
4 or law enforcement officer is located at the time the interception is
5 made.

6 (cf: P.L.1993,c.29,s.1)

7

8 3. Section 4 of P.L.1968, c.409 (C.2A:156A-4) is amended to read
9 as follows:

10 4. It shall not be unlawful under this act for:

11 a. An operator of a switchboard, or an officer, agent or employee
12 of a provider of wire or electronic communication service, whose
13 facilities are used in the transmission of a wire or electronic
14 communication, to intercept, disclose or use that communication in the
15 normal course of his employment while engaged in any activity which
16 is a necessary incident to the rendition of his service or to the
17 protection of the rights or property of the provider of that service. No
18 provider of wire or electronic communication service shall utilize
19 service observing or random monitoring except for mechanical or
20 service quality control checks;

21 b. Any investigative or law enforcement officer to intercept a wire,
22 electronic or oral communication, where such officer is a party to the
23 communication or where another officer who is a party to the
24 communication requests or requires him to make such interception;

25 c. Any person acting at the direction of an investigative or law
26 enforcement officer to intercept a wire, electronic or oral
27 communication, where such person is a party to the communication or
28 one of the parties to the communication has given prior consent to
29 such interception; provided, however, that no such interception shall
30 be made **【unless the】** without the prior approval of the Attorney
31 General or his designee or a county prosecutor **【within his authority**
32 **determines that there exists a reasonable suspicion that evidence of**
33 **criminal conduct will be derived from such interception】** or his
34 designee;

35 d. A person not acting under color of law to intercept a wire,
36 electronic or oral communication, where such person is a party to the
37 communication or one of the parties to the communication has given
38 prior consent to such interception unless such communication is
39 intercepted or used for the purpose of committing any criminal or
40 tortious act in violation of the Constitution or laws of the United
41 States or of this State or for the purpose of committing any other
42 injurious act. The fact that such person is the subscriber to a
43 particular telephone does not constitute consent effective to authorize
44 interception of communications among parties not including such
45 person on that telephone. Any person who unlawfully intercepts or
46 uses such communication as provided in this paragraph shall be subject

1 to the civil liability established in section 24 of P.L.1968, c.409
2 (C.2A:156A-24), in addition to any other criminal or civil liability
3 imposed by law;

4 e. Any person to intercept or access an electronic communication
5 made through an electronic communication system that is configured
6 so that such electronic communication is readily accessible to the
7 general public;

8 f. Any person to intercept any radio communication which is
9 transmitted:

10 (1) by any station for the use of the general public, or that relates
11 to ships, aircraft, vehicles, or persons in distress;

12 (2) by any governmental, law enforcement, civil defense, private
13 land mobile, or public safety communication system, including police
14 and fire, readily accessible to the general public;

15 (3) by a station operating on an authorized frequency within the
16 bands allocated to the amateur, citizens band, or general mobile radio
17 services; or

18 (4) by any marine or aeronautical communications system;

19 g. Any person to engage in any conduct which:

20 (1) is prohibited by section 633 of the Communications Act of
21 1934; or

22 (2) is excepted from the application of section 705(a) of the
23 Communications Act of 1934 by section 705(b) of that Act;

24 h. Any person to intercept any wire or electronic communication
25 the transmission of which is causing harmful interference to any
26 lawfully operating station or consumer electronic equipment, to the
27 extent necessary to identify the source of such interference; or for
28 other users of the same frequency to intercept any radio
29 communication made through a system that utilizes frequencies
30 monitored by individuals engaged in the provision or the use of such
31 system, if such communication is not scrambled or encrypted; or

32 i. A provider of [wire or] electronic communication service to
33 record the fact that a wire or electronic communication was initiated
34 or completed in order to protect such provider, another provider
35 furnishing service toward the completion of the wire or electronic
36 communication, or a user of that service, from fraudulent, unlawful or
37 abusive use of such service.

38 (cf: P.L.1993,c.29,s.3)

39

40 4. Section 8 of P.L.1968, c.409 (C.2A:156A-8) is amended to read
41 as follows:

42 8. The Attorney General, county prosecutor or a person
43 designated to act for such an official and to perform his duties in and
44 during his actual absence or disability, may authorize, in writing, an ex
45 parte application to a judge designated to receive the same for an
46 order authorizing the interception of a wire, or electronic or oral

1 communication by the investigative or law enforcement officers or
2 agency having responsibility for an investigation when such
3 interception may provide evidence of the commission of the offense of
4 murder, kidnapping, gambling, robbery, bribery, a violation of
5 paragraph (1) or (2) of subsection b. of N.J.S.2C:12-1, a violation of
6 section 3 of P.L. 1997, c.353 (C.2C:21-4.3), a violation of
7 N.J.S.2C:21-19 punishable by imprisonment for more than one year,
8 a violation of P.L.1994, c.121 (C.2C:21-23 et seq.), terroristic
9 threats, violations of N.J.S.2C:35-3, N.J.S.2C:35-4 and
10 N.J.S.2C:35-5, violations of sections 112 through 116, inclusive, of
11 the "Casino Control Act," P.L.1977, c.110 (C.5:12-112 through
12 5:12-116), arson, burglary, theft and related offenses punishable by
13 imprisonment for more than one year, endangering the welfare of a
14 child pursuant to N.J.S.2C:24-4, escape, forgery and fraudulent
15 practices punishable by imprisonment for more than one year,
16 alteration of motor vehicle identification numbers, unlawful
17 manufacture, purchase, use, or transfer of firearms, unlawful
18 possession or use of destructive devices or explosives, racketeering or
19 a violation of subsection g. of N.J.S.2C:5-2, leader of organized crime,
20 organized criminal activity directed toward the unlawful
21 transportation, storage, disposal, discharge, release, abandonment or
22 disposition of any harmful, hazardous, toxic, destructive, or polluting
23 substance, or any conspiracy to commit any of the foregoing offenses
24 or which may provide evidence aiding in the apprehension of the
25 perpetrator or perpetrators of any of the foregoing offenses.
26 (cf: P.L.1999, c.25, s.1)

27

28 5. Section 12 of P.L.1968, c.409 (C.2A:156A-12) is amended to
29 read as follows:

30 12. Each order authorizing the interception of any wire, electronic
31 or oral communication shall state:

32 a. The judge is authorized to issue the order;

33 b. The identity of, or a particular description of, the person, if
34 known, whose communications are to be intercepted;

35 c. The character and location of the particular communication
36 facilities as to which, or the particular place of the communication as
37 to which, authority to intercept is granted, or, in the case of an
38 application meeting the requirements of subsection g. of section 9 of
39 P.L.1968, c.409 (C.2A:156A-9) that specification is not practical or
40 that the purpose to thwart interception by changing facilities has been
41 shown;

42 d. A particular description of the type of the communication to be
43 intercepted and a statement of the particular offense to which it
44 relates;

45 e. The identity of the investigative or law enforcement officers or
46 agency to whom the authority to intercept a wire, electronic or oral

1 communication is given and the identity of whoever authorized the
2 application; and

3 f. The period of time during which such interception is authorized,
4 including a statement as to whether or not the interception shall
5 automatically terminate when the described communication has been
6 first obtained.

7 No order entered under this section shall authorize the interception
8 of any wire, electronic or oral communication for a period of time in
9 excess of that necessary under the circumstances. Every order entered
10 under this section shall require that such interception begin and
11 terminate as soon as practicable and be conducted in such a manner as
12 to minimize or eliminate the interception of such communications not
13 otherwise subject to interception under this act by making reasonable
14 efforts, whenever possible, to reduce the hours of interception
15 authorized by said order. In the event the intercepted communication
16 is in a language other than English, or is in a code, and an interpreter
17 or expert in that language or code is not reasonably available during
18 the interception period or a portion of the interception period,
19 minimization shall be accomplished as soon as practicable after the
20 interception. Except as provided below in subsection g. of this
21 section, no order entered under this section shall authorize the
22 interception of wire, electronic or oral communications for any period
23 exceeding 20 days. Extensions or renewals of such an order may be
24 granted for two additional periods of not more than 10 days. No
25 extension or renewal shall be granted unless an application for it is
26 made in accordance with this section, and the court makes the findings
27 required by sections 10 and 11 of P.L.1968, c.409 (C.2A:156A-10 and
28 2A:156A-11) and by this section.

29 g. Orders entered under this section to provide evidence of
30 racketeering in violation of N.J.S.2C:41-2, leader of organized crime
31 in violation of subsection g. of N.J.S.2C:5-2, or leader of narcotics
32 trafficking network in violation of N.J.S.2C:35-3, may authorize the
33 interception of wire, electronic or oral communications for a period
34 not to exceed 30 days and extensions or renewals of any order may be
35 granted for additional periods of not more than 30 days, without
36 limitation on the number of extension or renewal orders; provided,
37 however, that orders authorized pursuant to this subsection shall not
38 exceed six months.

39 h. Whenever an order authorizing an interception is entered, the
40 order may require reports to be made to the judge who issued the
41 order showing what progress has been made toward achievement of
42 the authorized objective and the need for continued interception. Such
43 reports shall be made at such intervals as the court may require.

44 An order authorizing the interception of a wire, electronic or oral
45 communication shall, upon request of the applicant, direct that a
46 provider of [wire or]electronic communication service shall furnish

1 the applicant forthwith all information, facilities and technical
2 assistance necessary to accomplish the interception unobtrusively and
3 with a minimum of interference with the services that such provider is
4 affording the person whose communications are to be intercepted.

5 The obligation of a provider of **[wire or]** electronic communication
6 service under such an order shall include but is not limited to
7 conducting an in-progress trace during an interception and shall also
8 include the provision of technical assistance and equipment and
9 utilization of any technological features which are available to the
10 provider of **[wire or]** electronic communication service. The
11 obligation of the provider of **[wire or]** electronic communication
12 service to conduct an in-progress trace and provide other technical
13 assistance may arise pursuant to court order based upon probable
14 cause, under circumstances not involving an interception pursuant to
15 this act. Any provider of **[wire or]** electronic communication service
16 furnishing such facilities or assistance shall be compensated therefor
17 by the applicant at the prevailing rates. Said provider shall be immune
18 from civil liability for any assistance rendered to the applicant pursuant
19 to this section.

20 An order authorizing the interception of a wire, electronic or oral
21 communication may be executed at any point of interception within
22 the jurisdiction of an investigative or law enforcement officer
23 executing the order.

24 (cf: P.L.1993,c.29,s.11)

25

26 6. Section 23 of P.L.1993, c.29 (C.2A:156A-29) is amended to
27 read as follows:

28 23. Requirements for access.

29 a. A law enforcement agency, but no other governmental entity,
30 may require the disclosure by a provider of **[wire or]** electronic
31 communication service or remote computing service of the contents of
32 an electronic communication without notice to the subscriber or the
33 customer if the law enforcement agency obtains a warrant.

34 b. Except as provided in subsection c. of this section, a provider
35 of electronic communication service or remote computing service may
36 disclose a record or other information pertaining to a subscriber or
37 customer of the service to any person other than a governmental
38 entity. This subsection shall not apply to the contents covered by
39 subsection a. of this section.

40 c. A provider of **[wire or]** electronic communication service or
41 remote computing service shall disclose a record or other information
42 pertaining to a subscriber or customer of the service, other than
43 contents covered by **[subsection]**subsections a. and f. of this section,
44 to a law enforcement agency under the following circumstances:

45 (1) the law enforcement agency has obtained a warrant; **[or]**

46 (2) the law enforcement agency has obtained the consent of the

1 subscriber or customer to the disclosure; or
2 (3) the law enforcement agency has obtained a court order for such
3 disclosure under subsection c. of this section.

4 A law enforcement agency receiving records or information
5 pursuant to this subsection is not required to provide notice to the
6 customer or subscriber.

7 d. Notwithstanding any other provision of law to the contrary, no
8 service provider, its officers, employees, agents or other specified
9 persons shall be liable in any civil action for damages as a result of
10 providing information, facilities or assistance in accordance with the
11 terms of a court order or warrant under this section.

12 e. A court order for disclosure under subsections b. or c. may be
13 issued by a judge of competent jurisdiction and shall issue only if the
14 law enforcement agency offers specific and articulable facts showing
15 that there are reasonable grounds to believe that the record or other
16 information pertaining to a subscriber or customer of an electronic
17 communication service or remote computing service is relevant and
18 material to an ongoing criminal investigation. A judge who has issued
19 an order pursuant to this section, on a motion made promptly by the
20 service provider, may quash or modify such order, if the information
21 or records requested are unusually voluminous in nature or compliance
22 with such order otherwise would cause an undue burden on such
23 provider.

24 f. A provider of electronic communication service or remote
25 computing service shall disclose to a law enforcement agency the
26 name, address, telephone number or other subscriber number or
27 identity, and length of service provided to a subscriber or customer of
28 such service and the types of services the subscriber or customer
29 utilized, when the law enforcement entity obtains a grand jury or trial
30 subpoena.

31 g. Upon the request of a law enforcement agency, a provider of
32 wire or electronic communication service or a remote computing
33 service shall take all necessary steps to preserve, for a period of 90
34 days, records and other evidence in its possession pending the issuance
35 of a warrant. The preservation period shall be extended for an
36 additional 90 days upon the request of the law enforcement agency.
37 (cf: P.L.1994,c.55,s.2)

38

39 7. This act shall take effect immediately .

40

41

42

STATEMENT

43

44 This bill amends the "New Jersey Wiretapping and Electronic
45 Surveillance Act" in order to address the problems facing law
46 enforcement agencies with regard to new technologies and to clarify

1 the procedures pertaining to the disclosure of information by the
2 providers to the law enforcement agencies.

3 The bill amends that provision of the act concerning ex-parte
4 orders. The act authorizes the Attorney General or a county
5 prosecutor to seek an ex-parte order allowing the interception of a
6 wire, electronic or oral communication for an investigation when the
7 investigation may provide evidence of the commission of an offense,
8 including but not limited to: murder, kidnapping, gambling, robbery
9 bribery, money laundering, terroristic threats, certain drug offenses,
10 violations of the "Casino Control Act," endangering the welfare of a
11 child or racketeering. This bill would expand the list to include health
12 care claims fraud, N.J.S.A. 2C:21-4.3. This bill would also clarify that
13 the list of enumerated offenses includes fraudulent practices punishable
14 by a term of imprisonment of more than one year.

15 Although the act requires that any order to intercept begin and
16 terminate as soon as practicable and that the interception be conducted
17 in a manner which minimizes the interception of communication not
18 otherwise subject to the order, there are instances when a law
19 enforcement agency may be faced with the situation where the
20 intercepted communication is in a language other than English or is
21 in code. If this is the case and an interpreter or expert is not available
22 during the interception period, the bill requires that the minimized
23 interception must be accomplished as soon as practicable. These
24 requirements are consistent with federal law. In addition, the bill
25 provides that an order authorizing interception may be executed at any
26 point of interception within the jurisdiction of an investigative or law
27 enforcement officer executing the order. The bill defines "point of
28 interception" as the site at which the investigative or law enforcement
29 officer is located at the time the interception is made.

30 This bill would also amend that provision of the act concerning the
31 disclosure by a provider of electronic communication service or
32 remote computing service to a law enforcement agency of the
33 contents of a subscriber's or customer's communication or the
34 disclosure of a subscriber's or customer's information. The act
35 provides that a law enforcement officer who has obtained a warrant
36 may require a provider to disclose the contents of a communication
37 without providing notice to the subscriber or the customer. The act
38 also provides that a provider shall disclose a record or other
39 information pertaining to a subscriber or customer of the service, other
40 than the contents of the communication, provided the law
41 enforcement agency obtains a warrant or consent from the subscriber
42 or customer. This bill would amend this section of the act to
43 authorize the provider to disclose the information if the law
44 enforcement agency obtained an order for disclosure. An order for
45 disclosure may be issued by a judge only if the law enforcement
46 agency offers specific and articulable facts showing that there are

1 reasonable grounds to believe that the record or other information
2 pertaining to a subscriber or customer of a service is relevant and
3 material to an ongoing criminal investigation. The judge who has
4 issued such an order may quash or modify the order, on a motion by
5 the service provider, if the information or records requested are
6 unusually voluminous in nature or compliance with such an order
7 would otherwise cause an undue burden on the provider. This bill also
8 requires a provider to disclose to a law enforcement agency, when the
9 law enforcement entity obtains a grand jury or trial subpoena, such
10 information as: the subscriber's name, address, telephone number or
11 other number or identity, the length of service provided and the types
12 of services utilized by the subscriber. In addition, the bill provides
13 that, upon the request of a law enforcement agency, a provider shall
14 take all necessary steps to preserve, for a period of 90 days, records
15 and other evidence in its possession pending the issuance of a warrant.
16 The preservation period shall be extended for an additional 90 days
17 upon the request of the law enforcement agency.

18 The bill also implements a technical change for consistency with the
19 federal law by deleting several references to wire communication
20 service. Wire communication service is included within the definition
21 of electronic communication service. Hence, these changes are not
22 intended to and do not make any substantive changes to the act.

23 In addition, this bill would eliminate the sunset provision, making
24 the act permanent. Currently, the act has a sunset provision which
25 requires the Legislature to re-authorize the act every several years.
26 The act is due to expire on July 1, 1999.

ASSEMBLY JUDICIARY COMMITTEE

STATEMENT TO

ASSEMBLY, No. 3014

STATE OF NEW JERSEY

DATED: MARCH 25, 1999

The Assembly Judiciary Committee reports favorably Assembly Bill No. 3014.

This bill amends the "New Jersey Wiretapping and Electronic Surveillance Act."

EX PARTE ORDERS. The bill amends the wiretapping act concerning ex-parte orders. The act authorizes the Attorney General or county prosecutor to seek an ex-parte order allowing interception of a communication for an investigation which may provide evidence of the commission of specified offenses, including, for example, murder, kidnapping, gambling, robbery bribery, money laundering, terroristic threats, certain drug offenses, violations of the "Casino Control Act," endangering the welfare of a child or racketeering. This bill would expand the list to include health care claims fraud, N.J.S.A.2C:21-4.3 and fraudulent practices punishable by a term of imprisonment for more than one year.

MINIMIZATION OF INTERCEPTION. Although the act requires that any order to intercept begin and terminate as soon as practicable and the interception be conducted in a manner which minimizes the interception of communication not otherwise subject to the order, a law enforcement agency may be faced with the situation where the intercepted communication is in a language other than English or is in code. If this is the case and an interpreter or expert is not available during the interception period, the bill requires that the minimized interception be accomplished as soon as practicable. These requirements are consistent with federal law.

POINT OF INTERCEPTION. The bill provides that an order authorizing interception may be executed at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order. The bill defines "point of interception" as the site at which the investigative or law enforcement officer is located at the time the interception is made.

REQUIREMENTS OF ACCESS FOR DISCLOSURE. This bill would also amend the act concerning the requirements of access for disclosure by a provider of electronic communication service or remote computing service to a law enforcement agency of a subscriber's or customer's information or the contents of a

communication of a subscriber or customer.

The act currently provides that a law enforcement officer who has obtained a warrant may require a provider to disclose the contents of a communication without providing notice to the subscriber or the customer. The bill includes remote computing service in this provision. The probable cause search warrant is the most stringent requirement for access.

This bill requires a provider to disclose to a law enforcement agency, when the law enforcement entity obtains a grand jury or trial subpoena, such information as: the subscriber's name, address, telephone number or other number or identity, the length of service provided and the types of services utilized by the subscriber. The subpoena would be the least stringent requirement for access.

The act also currently includes that a provider shall disclose a record or other information pertaining to a subscriber or customer, other than the contents of a communication, provided the law enforcement agency obtains a warrant or consent from the subscriber or customer. This bill would authorize a third option; the provider would disclose the information if the law enforcement agency obtained an order for disclosure. An order for disclosure may be issued by a judge only if the law enforcement agency offers specific and articulable facts showing reasonable grounds to believe that the record or other information pertaining to a subscriber or customer is relevant and material to an ongoing criminal investigation. The judge who issues such an order may quash or modify the order, on a motion by the service provider, if the information or records requested are unusually voluminous or compliance with such an order would cause an undue burden on the provider.

The bill provides that, upon the request of a law enforcement agency, a provider shall take all necessary steps to preserve, for a period of 90 days, records and other evidence in its possession pending the issuance of a warrant. The preservation period shall be extended for an additional 90 days upon the request of the law enforcement agency.

The bill also implements a technical change for consistency with the federal law by omitting "wire" in reference to "provider of wire or electronic communication service" since wire communication service is included within the definition of electronic communication service. These changes are not intended to make any substantive changes to the act.

ACT TO BE PERMANENT. This bill would make the wiretapping act permanent by eliminating the sunset provision. Currently, the act has a sunset provision which requires the Legislature to re-authorize the act every several years. The act is due to expire on July 1, 1999.

SENATE JUDICIARY COMMITTEE

STATEMENT TO

ASSEMBLY, No. 3014

STATE OF NEW JERSEY

DATED: JUNE 7, 1999

The Senate Judiciary Committee reports favorably Assembly Bill No. 3014.

This bill proposes a series of amendments to the New Jersey Wiretapping and Electronic Surveillance Act. The following is a brief description of those amendments.

1. Presently, the act has a sunset provision which requires the Legislature to periodically re-authorize the act. The current authorization is set to expire on July 1, 1999. This bill would make the wiretapping act permanent by eliminating the sunset provision.

2. The act presently authorizes the Attorney General or county prosecutor to seek an ex-parte order allowing interception of a communication for an investigation which may provide evidence of the commission of specified offenses, including, for example, murder, kidnaping, gambling, robbery, bribery, money laundering, terroristic threats, certain drug offenses, violations of the "Casino Control Act," endangering the welfare of a child and racketeering. This bill would expand the list to include health care fraud claims and fraudulent practices punishable by a term of imprisonment of more than one year.

3. While the act requires that any order to intercept begin and terminate as soon as practicable and that the interception be conducted in a manner which minimizes the interception of communication not otherwise subject to the court order, a law enforcement agency may be faced with the situation where the intercepted communication is in a language other than English or is in code. If this is the case and an interpreter or expert is not available during the interception period, the bill requires that the minimized interception be accomplished as soon as practicable. This requirement is consistent with federal law.

4. The bill provides that an order authorizing interception may be executed at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order. The bill defines "point of interception" as the site at which the investigative or law enforcement officer is located at the time the interception is made.

5. The act currently provides that a law enforcement officer who has obtained a warrant may require a provider of electronic communication service to disclose the contents of a communication without providing notice to the subscriber or the customer. The bill includes remote computing service providers in this provision. The bill

also requires a provider to disclose to a law enforcement agency, when the law enforcement entity obtains a grand jury or trial subpoena, information such as: the subscriber's name, address, telephone number or other number or identity, the length of service provided and the types of services utilized by the subscriber.

6. The act also currently requires that a provider disclose a record or other information pertaining to a subscriber or customer, other than the contents of a communication, provided the law enforcement agency obtains a warrant or consent from the subscriber or customer. The bill would authorize a third option: the provider would be required to disclose the information if the law enforcement agency obtained an order for disclosure. An order for disclosure may be issued by a judge only if the law enforcement agency offers specific and articulable facts showing reasonable grounds to believe that the record or other information pertaining to a subscriber or customer is relevant and material to an ongoing criminal investigation. The judge who issues such an order may quash or modify the order, on a motion by the service provider, if the information or records requested are unusually voluminous or compliance with such an order would cause an undue burden on the provider.

7. The bill provides that, upon request of a law enforcement agency, a provider shall take all necessary steps to preserve, for a period of 90 days, records and other evidence in its possession pending the issuance of a warrant. The preservation period shall be extended for an additional 90 days upon the request of the law enforcement agency.

8. The bill also implement a technical change for consistency with the federal law by omitting "wire" in reference to "provider of wire or electronic communication service" since wire communication service is included within the definition of electronic communication service. These changes are not intended to make any substantive changes to the act.

LEGISLATIVE FISCAL ESTIMATE

[CORRECTED COPY]

ASSEMBLY, No. 3014

STATE OF NEW JERSEY

208th LEGISLATURE

DATED: JUNE 23, 1999

Corrected Copy Assembly Bill No. 3014 of 1999 amends and makes permanent the "New Jersey Wiretapping and Electronic Surveillance Act" in order to address the problems facing law enforcement agencies with regard to new technologies and to clarify the procedures pertaining to the disclosure of information by providers of electronic communication service or remote computing service to the law enforcement agencies. Specifically, the bill would expand the wiretapping act to authorize ex-parte orders for investigations related to health care claims fraud, N.J.S.A.2C:21-4.3 and fraudulent practices punishable by a term of imprisonment for more than one year. The bill would also permit an order authorizing interception to be executed at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order. This bill would also require a provider to disclose to a law enforcement agency, pursuant to a grand jury or trial subpoena, information such as the subscriber's name, address, telephone number and the types of services utilized by the subscriber.

The Department of Law and Public Safety informally indicates that this bill would not have an appreciable fiscal impact on the State or its localities. The department notes that the Division of Criminal Justice's organized crime unit is adequately staffed to advise law enforcement officials concerning changes to current law and that most law enforcement agencies presently have the surveillance equipment necessary to implement the bill's provisions.

The Office of Legislative Services concurs with this estimate but notes that by expanding the scope of cases in which wiretaps may be used, the bill could increase the cost of certain criminal investigations.

This fiscal estimate has been prepared pursuant to P.L.1980, c.67.

SENATE, No. 1858

STATE OF NEW JERSEY
208th LEGISLATURE

INTRODUCED MAY 10, 1999

Sponsored by:

Senator LOUIS F. KOSCO

District 38 (Bergen)

Senator JOHN J. MATHEUSSEN

District 4 (Camden and Gloucester)

Co-Sponsored by:

Senators Allen and Bucco

SYNOPSIS

Amends the "New Jersey Wiretapping and Electronic Surveillance Act."

CURRENT VERSION OF TEXT

As introduced.



(Sponsorship Updated As Of: 5/21/1999)

1 AN ACT concerning wiretapping and electronic surveillance and
2 amending P.L.1968, c.409 and P.L.1993, c.29.

3
4 **BE IT ENACTED** by the Senate and General Assembly of the State
5 of New Jersey:

6
7 1. Section 28 of P.L.1968, c.409 is amended to read as follows:

8 28. This act shall take effect January 1, 1969 **[and remain in effect**
9 **until July 1, 1999]**.
10 (cf: P.L.1994, c.55, s.1)

11

12 2. Section 2 of P.L.1968, c.409 (C.2A:156A-2) is amended to read
13 as follows:

14 2. As used in this act:

15 a. "Wire communication" means any aural transfer made in whole
16 or in part through the use of facilities for the transmission of
17 communications by the aid of wire, cable or other like connection
18 between the point of origin and the point of reception, including the
19 use of such connection in a switching station, furnished or operated by
20 any person engaged in providing or operating such facilities for the
21 transmission of intrastate, interstate or foreign communication. "Wire
22 communication" includes any electronic storage of such
23 communication, and the radio portion of a cordless telephone
24 communication that is transmitted between the cordless telephone
25 handset and the base unit;

26 b. "Oral communication" means any oral communication uttered
27 by a person exhibiting an expectation that such communication is not
28 subject to interception under circumstances justifying such
29 expectation, but does not include any electronic communication;

30 c. "Intercept" means the aural or other acquisition of the contents
31 of any wire, electronic or oral communication through the use of any
32 electronic, mechanical, or other device;

33 d. "Electronic, mechanical or other device" means any device or
34 apparatus, including an induction coil, that can be used to intercept a
35 wire, electronic or oral communication other than:

36 (1) Any telephone or telegraph instrument, equipment or facility,
37 or any component thereof, furnished to the subscriber or user by a
38 provider of wire or electronic communication service in the ordinary
39 course of its business and being used by the subscriber or user in the
40 ordinary course of its business; or furnished by such subscriber or user
41 for connection to the facilities of such service and used in the ordinary
42 course of its business; or being used by a provider of wire or electronic
43 communication service in the ordinary course of its business, or by an

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

- 1 investigative or law enforcement officer in the ordinary course of his
2 duties; or
- 3 (2) A hearing aid or similar device being used to correct subnormal
4 hearing to not better than normal;
- 5 e. "Person" means that term as defined in R.S.1:1-2 and includes
6 any officer or employee of the State or of a political subdivision
7 thereof;
- 8 f. "Investigative or law enforcement officer" means any officer of
9 the State of New Jersey or of a political subdivision thereof who is
10 empowered by law to conduct investigations of, or to make arrests for,
11 any offense enumerated in section 8 of P.L.1968, c.409
12 (C.2A:156A-8) and any attorney authorized by law to prosecute or
13 participate in the prosecution of any such offense;
- 14 g. "Contents," when used with respect to any wire, electronic or
15 oral communication, includes any information concerning the identity
16 of the parties to such communication or the existence, substance,
17 purport, or meaning of that communication, except that for purposes
18 of sections 22, 23, 24 and 26 of P.L.1993, c.29 (C.2A:156A-28,
19 C.2A:156A-29, C.2A:156A-30, and C.2A:156A-32) contents, when
20 used with respect to any wire, electronic, or oral communication
21 means any information concerning the substance, purport or meaning
22 of that communication;
- 23 h. "Court of competent jurisdiction" means the Superior Court;
- 24 i. "Judge," when referring to a judge authorized to receive
25 applications for, and to enter, orders authorizing interceptions of wire,
26 electronic or oral communications, means one of the several judges of
27 the Superior Court to be designated from time to time by the Chief
28 Justice of the Supreme Court to receive applications for, and to enter,
29 orders authorizing interceptions of wire, electronic or oral
30 communications pursuant to this act;
- 31 j. "Communication common carrier" means any person engaged as
32 a common carrier for hire, in intrastate, interstate or foreign
33 communication by wire or radio or in intrastate, interstate or foreign
34 radio transmission of energy; but a person engaged in radio
35 broadcasting shall not, while so engaged, be deemed a common
36 carrier;
- 37 k. "Aggrieved person" means a person who was a party to any
38 intercepted wire, electronic or oral communication or a person against
39 whom the interception was directed;
- 40 l. "In-progress trace" means the determination of the origin of a
41 telephonic communication to a known telephone during the
42 communication;
- 43 m. "Electronic communication" means any transfer of signs,
44 signals, writing, images, sounds, data, or intelligence of any nature
45 transmitted in whole or in part by a wire, radio, electromagnetic,
46 photoelectric or photo-optical system that affects interstate, intrastate

- 1 or foreign commerce, but does not include:
- 2 (1) Any wire or oral communication;
- 3 (2) Any communication made through a tone-only paging device;
- 4 or
- 5 (3) Any communication from a tracking device;
- 6 n. "User" means any person or entity who:
- 7 (1) Uses an electronic communication service; and
- 8 (2) Is duly authorized by the provider of such service to engage in
- 9 such use;
- 10 o. "Electronic communication system" means any wire, radio,
- 11 electromagnetic, photo-optical or photoelectronic facilities for the
- 12 transmission of electronic communications, and any computer facilities
- 13 or related electronic equipment for the electronic storage of such
- 14 communications;
- 15 p. "Electronic communication service" means any service which
- 16 provides to the users thereof the ability to send or receive wire or
- 17 electronic communications;
- 18 q. "Electronic storage" means:
- 19 (1) Any temporary, intermediate storage of a wire or electronic
- 20 communication incidental to the electronic transmission thereof; and
- 21 (2) Any storage of such communication by an electronic
- 22 communication service for purpose of backup protection of the
- 23 communication;
- 24 r. "Readily accessible to the general public" means, with respect
- 25 to a radio communication, that such communication is not:
- 26 (1) Scrambled or encrypted;
- 27 (2) Transmitted using modulation techniques whose essential
- 28 parameters have been withheld from the public with the intention of
- 29 preserving the privacy of such communication;
- 30 (3) Carried on a subcarrier or other signal subsidiary to a radio
- 31 transmission;
- 32 (4) Transmitted over a communication system provided by a
- 33 common carrier, unless the communication is a tone-only paging
- 34 system communication; or
- 35 (5) Transmitted on frequencies allocated under part 25, subpart D,
- 36 E, or F of part 74, or part 94 of the Rules of the Federal
- 37 Communications Commission, unless, in the case of a communication
- 38 transmitted on a frequency allocated under part 74 that is not
- 39 exclusively allocated to broadcast auxiliary services, the
- 40 communication is a two-way voice communication by radio;
- 41 s. "Remote computing service" means the provision to the public
- 42 of computer storage or processing services by means of an electronic
- 43 communication system;
- 44 t. "Aural transfer" means a transfer containing the human voice at
- 45 any point between and including the point of origin and the point of
- 46 reception;

1 u. "Tracking device" means an electronic or mechanical device
2 which permits the tracking of the movement of a person or device;

3 v. "Point of interception" means the site at which the investigative
4 or law enforcement officer is located at the time the interception is
5 made.

6 (cf: P.L.1993,c.29,s.1)

7

8 3. Section 4 of P.L.1968, c.409 (C.2A:156A-4) is amended to read
9 as follows:

10 4. It shall not be unlawful under this act for:

11 a. An operator of a switchboard, or an officer, agent or employee
12 of a provider of wire or electronic communication service, whose
13 facilities are used in the transmission of a wire or electronic
14 communication, to intercept, disclose or use that communication in the
15 normal course of his employment while engaged in any activity which
16 is a necessary incident to the rendition of his service or to the
17 protection of the rights or property of the provider of that service. No
18 provider of wire or electronic communication service shall utilize
19 service observing or random monitoring except for mechanical or
20 service quality control checks;

21 b. Any investigative or law enforcement officer to intercept a wire,
22 electronic or oral communication, where such officer is a party to the
23 communication or where another officer who is a party to the
24 communication requests or requires him to make such interception;

25 c. Any person acting at the direction of an investigative or law
26 enforcement officer to intercept a wire, electronic or oral
27 communication, where such person is a party to the communication or
28 one of the parties to the communication has given prior consent to
29 such interception; provided, however, that no such interception shall
30 be made **【unless the】** without the prior approval of the Attorney
31 General or his designee or a county prosecutor **【within his authority**
32 **determines that there exists a reasonable suspicion that evidence of**
33 **criminal conduct will be derived from such interception】** or his
34 designee;

35 d. A person not acting under color of law to intercept a wire,
36 electronic or oral communication, where such person is a party to the
37 communication or one of the parties to the communication has given
38 prior consent to such interception unless such communication is
39 intercepted or used for the purpose of committing any criminal or
40 tortious act in violation of the Constitution or laws of the United
41 States or of this State or for the purpose of committing any other
42 injurious act. The fact that such person is the subscriber to a
43 particular telephone does not constitute consent effective to authorize
44 interception of communications among parties not including such
45 person on that telephone. Any person who unlawfully intercepts or
46 uses such communication as provided in this paragraph shall be subject

1 to the civil liability established in section 24 of P.L.1968, c.409
2 (C.2A:156A-24), in addition to any other criminal or civil liability
3 imposed by law;

4 e. Any person to intercept or access an electronic communication
5 made through an electronic communication system that is configured
6 so that such electronic communication is readily accessible to the
7 general public;

8 f. Any person to intercept any radio communication which is
9 transmitted:

10 (1) by any station for the use of the general public, or that relates
11 to ships, aircraft, vehicles, or persons in distress;

12 (2) by any governmental, law enforcement, civil defense, private
13 land mobile, or public safety communication system, including police
14 and fire, readily accessible to the general public;

15 (3) by a station operating on an authorized frequency within the
16 bands allocated to the amateur, citizens band, or general mobile radio
17 services; or

18 (4) by any marine or aeronautical communications system;

19 g. Any person to engage in any conduct which:

20 (1) is prohibited by section 633 of the Communications Act of
21 1934; or

22 (2) is excepted from the application of section 705(a) of the
23 Communications Act of 1934 by section 705(b) of that Act;

24 h. Any person to intercept any wire or electronic communication
25 the transmission of which is causing harmful interference to any
26 lawfully operating station or consumer electronic equipment, to the
27 extent necessary to identify the source of such interference; or for
28 other users of the same frequency to intercept any radio
29 communication made through a system that utilizes frequencies
30 monitored by individuals engaged in the provision or the use of such
31 system, if such communication is not scrambled or encrypted; or

32 i. A provider of **【wire or】** electronic communication service to
33 record the fact that a wire or electronic communication was initiated
34 or completed in order to protect such provider, another provider
35 furnishing service toward the completion of the wire or electronic
36 communication, or a user of that service, from fraudulent, unlawful or
37 abusive use of such service.

38 (cf: P.L.1993,c.29,s.3)

39

40 4. Section 8 of P.L.1968, c.409 (C.2A:156A-8) is amended to read
41 as follows:

42 8. The Attorney General, county prosecutor or a person
43 designated to act for such an official and to perform his duties in and
44 during his actual absence or disability, may authorize, in writing, an ex
45 parte application to a judge designated to receive the same for an
46 order authorizing the interception of a wire, or electronic or oral

1 communication by the investigative or law enforcement officers or
2 agency having responsibility for an investigation when such
3 interception may provide evidence of the commission of the offense of
4 murder, kidnapping, gambling, robbery, bribery, a violation of
5 paragraph (1) or (2) of subsection b. of N.J.S.2C:12-1, a violation of
6 section 3 of P.L.1997,c.353 (C.2C:21-4.3), a violation of
7 N.J.S.2C:21-19 punishable by imprisonment for more than one year,
8 a violation of P.L.1994, c.121 (C.2C:21-23 et seq.), terroristic
9 threats, violations of N.J.S.2C:35-3, N.J.S.2C:35-4 and
10 N.J.S.2C:35-5, violations of sections 112 through 116, inclusive, of
11 the "Casino Control Act," P.L.1977, c.110 (C.5:12-112 through
12 5:12-116), arson, burglary, theft and related offenses punishable by
13 imprisonment for more than one year, endangering the welfare of a
14 child pursuant to N.J.S.2C:24-4, escape, forgery and fraudulent
15 practices punishable by imprisonment for more than one year,
16 alteration of motor vehicle identification numbers, unlawful
17 manufacture, purchase, use, or transfer of firearms, unlawful
18 possession or use of destructive devices or explosives, racketeering or
19 a violation of subsection g. of N.J.S.2C:5-2, leader of organized crime,
20 organized criminal activity directed toward the unlawful
21 transportation, storage, disposal, discharge, release, abandonment or
22 disposition of any harmful, hazardous, toxic, destructive, or polluting
23 substance, or any conspiracy to commit any of the foregoing offenses
24 or which may provide evidence aiding in the apprehension of the
25 perpetrator or perpetrators of any of the foregoing offenses.

26 (cf: P.L.1999, c.25, s.1)

27

28 5. Section 12 of P.L.1968, c.409 (C.2A:156A-12) is amended to
29 read as follows:

30 12. Each order authorizing the interception of any wire, electronic
31 or oral communication shall state:

32 a. The judge is authorized to issue the order;

33 b. The identity of, or a particular description of, the person, if
34 known, whose communications are to be intercepted;

35 c. The character and location of the particular communication
36 facilities as to which, or the particular place of the communication as
37 to which, authority to intercept is granted, or, in the case of an
38 application meeting the requirements of subsection g. of section 9 of
39 P.L.1968, c.409 (C.2A:156A-9) that specification is not practical or
40 that the purpose to thwart interception by changing facilities has been
41 shown;

42 d. A particular description of the type of the communication to be
43 intercepted and a statement of the particular offense to which it
44 relates;

45 e. The identity of the investigative or law enforcement officers or
46 agency to whom the authority to intercept a wire, electronic or oral

1 communication is given and the identity of whoever authorized the
2 application; and

3 f. The period of time during which such interception is authorized,
4 including a statement as to whether or not the interception shall
5 automatically terminate when the described communication has been
6 first obtained.

7 No order entered under this section shall authorize the interception
8 of any wire, electronic or oral communication for a period of time in
9 excess of that necessary under the circumstances. Every order entered
10 under this section shall require that such interception begin and
11 terminate as soon as practicable and be conducted in such a manner as
12 to minimize or eliminate the interception of such communications not
13 otherwise subject to interception under this act by making reasonable
14 efforts, whenever possible, to reduce the hours of interception
15 authorized by said order. In the event the intercepted communication
16 is in a language other than English, or is in a code, and an interpreter
17 or expert in that language or code is not reasonably available during
18 the interception period or a portion of the interception period,
19 minimization shall be accomplished as soon as practicable after the
20 interception. Except as provided below in subsection g. of this
21 section, no order entered under this section shall authorize the
22 interception of wire, electronic or oral communications for any period
23 exceeding 20 days. Extensions or renewals of such an order may be
24 granted for two additional periods of not more than 10 days. No
25 extension or renewal shall be granted unless an application for it is
26 made in accordance with this section, and the court makes the findings
27 required by sections 10 and 11 of P.L.1968, c.409 (C.2A:156A-10 and
28 2A:156A-11) and by this section.

29 g. Orders entered under this section to provide evidence of
30 racketeering in violation of N.J.S.2C:41-2, leader of organized crime
31 in violation of subsection g. of N.J.S.2C:5-2, or leader of narcotics
32 trafficking network in violation of N.J.S.2C:35-3, may authorize the
33 interception of wire, electronic or oral communications for a period
34 not to exceed 30 days and extensions or renewals of any order may be
35 granted for additional periods of not more than 30 days, without
36 limitation on the number of extension or renewal orders; provided,
37 however, that orders authorized pursuant to this subsection shall not
38 exceed six months.

39 h. Whenever an order authorizing an interception is entered, the
40 order may require reports to be made to the judge who issued the
41 order showing what progress has been made toward achievement of
42 the authorized objective and the need for continued interception. Such
43 reports shall be made at such intervals as the court may require.

44 An order authorizing the interception of a wire, electronic or oral
45 communication shall, upon request of the applicant, direct that a
46 provider of [wire or]electronic communication service shall furnish

1 the applicant forthwith all information, facilities and technical
2 assistance necessary to accomplish the interception unobtrusively and
3 with a minimum of interference with the services that such provider is
4 affording the person whose communications are to be intercepted.

5 The obligation of a provider of **【wire or】** electronic communication
6 service under such an order shall include but is not limited to
7 conducting an in-progress trace during an interception and shall also
8 include the provision of technical assistance and equipment and
9 utilization of any technological features which are available to the
10 provider of **【wire or 】** electronic communication service. The
11 obligation of the provider of **【wire or】** electronic communication
12 service to conduct an in-progress trace and provide other technical
13 assistance may arise pursuant to court order based upon probable
14 cause, under circumstances not involving an interception pursuant to
15 this act. Any provider of **【wire or】** electronic communication service
16 furnishing such facilities or assistance shall be compensated therefor
17 by the applicant at the prevailing rates. Said provider shall be immune
18 from civil liability for any assistance rendered to the applicant pursuant
19 to this section.

20 An order authorizing the interception of a wire, electronic or oral
21 communication may be executed at any point of interception within
22 the jurisdiction of an investigative or law enforcement officer
23 executing the order.

24 (cf: P.L.1993,c.29,s.11)

25

26 6. Section 23 of P.L.1993, c.29 (C.2A:156A-29) is amended to
27 read as follows:

28 23. Requirements for access. a. A law enforcement agency, but
29 no other governmental entity, may require the disclosure by a provider
30 of **【wire or】** electronic communication service or remote computing
31 service of the contents of an electronic communication without notice
32 to the subscriber or the customer if the law enforcement agency
33 obtains a warrant.

34 b. Except as provided in subsection c. of this section, a provider
35 of electronic communication service or remote computing service may
36 disclose a record or other information pertaining to a subscriber or
37 customer of the service to any person other than a governmental
38 entity. This subsection shall not apply to the contents covered by
39 subsection a. of this section.

40 c. A provider of **【wire or】** electronic communication service or
41 remote computing service shall disclose a record or other information
42 pertaining to a subscriber or customer of the service, other than
43 contents covered by **【subsection】**subsections a. and f. of this section,
44 to a law enforcement agency under the following circumstances:

45 (1) the law enforcement agency has obtained a warrant; **【or】**

46 (2) the law enforcement agency has obtained the consent of the

1 subscriber or customer to the disclosure; or
2 (3) the law enforcement agency has obtained a court order for such
3 disclosure under subsection (e) of this section.

4 A law enforcement agency receiving records or information
5 pursuant to this subsection is not required to provide notice to the
6 customer or subscriber.

7 d. Notwithstanding any other provision of law to the contrary, no
8 service provider, its officers, employees, agents or other specified
9 persons shall be liable in any civil action for damages as a result of
10 providing information, facilities or assistance in accordance with the
11 terms of a court order or warrant under this section.

12 e. A court order for disclosure under subsections (b) or (c) may
13 be issued by a judge of competent jurisdiction and shall issue only if
14 the law enforcement agency offers specific and articulable facts
15 showing that there are reasonable grounds to believe that the record
16 or other information pertaining to a subscriber or customer of an
17 electronic communication service or remote computing service is
18 relevant and material to an ongoing criminal investigation. A judge
19 who has issued an order pursuant to this section, on a motion made
20 promptly by the service provider, may quash or modify such order, if
21 the information or records requested are unusually voluminous in
22 nature or compliance with such order otherwise would cause an undue
23 burden on such provider.

24 f. A provider of electronic communication service or remote
25 computing service shall disclose to a law enforcement agency the
26 name, address, telephone number or other subscriber number or
27 identity, and length of service provided to a subscriber or customer of
28 such service and the types of services the subscriber or customer
29 utilized, when the law enforcement entity obtains a grand jury or trial
30 subpoena.

31 g. Upon the request of a law enforcement agency, a provider of
32 wire or electronic communication services or a remote computing
33 service shall take all necessary steps to preserve, for a period of 90
34 days, records and other evidence in its possession pending the issuance
35 of a warrant. The preservation period shall be extended for an
36 additional 90 days upon the request of the law enforcement agency.
37 (cf: P.L.1994,c.55,s.2)

38

39 7. This act shall take effect immediately .

40

41

42 STATEMENT

43

44 This bill amends the "New Jersey Wiretapping and Electronic
45 Surveillance Act" in order to address the problems facing law
46 enforcement agencies with regard to new technologies and to clarify

1 the procedures pertaining to the disclosure of information by the
2 providers to the law enforcement agencies.

3 The bill amends that provision of the act concerning ex-parte
4 orders. The act authorizes the Attorney General or a county
5 prosecutor to seek an ex-parte order allowing the interception of a
6 wire, electronic or oral communication for an investigation when the
7 investigation may provide evidence of the commission of an offense,
8 including but not limited to: murder, kidnapping, gambling, robbery
9 bribery, money laundering, terroristic threats, certain drug offenses,
10 violations of the "Casino Control Act," endangering the welfare of a
11 child or racketeering. This bill would expand the list to include health
12 care claims fraud, N.J.S.A.2C:21-4.3. This bill would also clarify that
13 the list of enumerated offenses includes fraudulent practices punishable
14 by a term of imprisonment of more than one year.

15 Although the act requires that any order to intercept begin and
16 terminate as soon as practicable and that the interception be conducted
17 in a manner which minimizes the interception of communication not
18 otherwise subject to the order, there are instances when a law
19 enforcement agency may be faced with the situation where the
20 intercepted communication is in a language other than English or is
21 in code. If this is the case and an interpreter or expert is not available
22 during the interception period, the bill requires that the minimized
23 interception must be accomplished as soon as practicable. These
24 requirements are consistent with federal law. In addition, the bill
25 provides that an order authorizing interception may be executed at any
26 point of interception within the jurisdiction of an investigative or law
27 enforcement officer executing the order. The bill defines "point of
28 interception" as the site at which the investigative or law enforcement
29 officer is located at the time the interception is made.

30 This bill would also amend that provision of the act concerning the
31 disclosure by a provider of electronic communication service or
32 remote computing service to a law enforcement agency of the
33 contents of a subscriber's or customer's communication or the
34 disclosure of a subscriber's or customer's information. The act
35 provides that a law enforcement officer who has obtained a warrant
36 may require a provider to disclose the contents of a communication
37 without providing notice to the subscriber or the customer. The act
38 also provides that a provider shall disclose a record or other
39 information pertaining to a subscriber or customer of the service, other
40 than the contents of the communication, provided the law
41 enforcement agency obtains a warrant or consent from the subscriber
42 or customer. This bill would amend this section of the act to
43 authorize the provider to disclose the information if the law
44 enforcement agency obtained an order for disclosure. An order for
45 disclosure may be issued by a judge only if the law enforcement
46 agency offers specific and articulable facts showing that there are

1 reasonable grounds to believe that the record or other information
2 pertaining to a subscriber or customer of a service is relevant and
3 material to an ongoing criminal investigation. The judge who has
4 issued such an order may quash or modify the order, on a motion by
5 the service provider, if the information or records requested are
6 unusually voluminous in nature or compliance with such an order
7 would otherwise cause an undue burden on the provider. This bill also
8 requires a provider to disclose to a law enforcement agency, when the
9 law enforcement entity obtains a grand jury or trial subpoena, such
10 information as: the subscriber's name, address, telephone number or
11 other number or identity, the length of service provided and the types
12 of services utilized by the subscriber. In addition, the bill provides
13 that, upon the request of a law enforcement agency, a provider shall
14 take all necessary steps to preserve, for a period of 90 days, records
15 and other evidence in its possession pending the issuance of a warrant.
16 The preservation period shall be extended for an additional 90 days
17 upon the request of the law enforcement agency.

18 The bill also implements a technical change for consistency with the
19 federal law by deleting several references to wire communication
20 service. Wire communication service is included within the definition
21 of electronic communication service. Hence, these changes are not
22 intended to and do not make any substantive changes to the act.

23 In addition, this bill would eliminate the sunset provision, making
24 the act permanent. Currently, the act has a sunset provision which
25 requires the Legislature to re-authorize the act every several years.
26 The act is due to expire on July 1, 1999.

SENATE JUDICIARY COMMITTEE

STATEMENT TO

SENATE, No. 1858

STATE OF NEW JERSEY

DATED: JUNE 7, 1999

The Senate Judiciary Committee reports favorably Senate Bill No. 1858.

This bill proposes a series of amendments to the New Jersey Wiretapping and Electronic Surveillance Act. The following is a brief description of those amendments.

1. Presently, the act has a sunset provision which requires the Legislature to periodically re-authorize the act. The current authorization is set to expire on July 1, 1999. This bill would make the wiretapping act permanent by eliminating the sunset provision.

2. The act presently authorizes the Attorney General or county prosecutor to seek an ex-parte order allowing interception of a communication for an investigation which may provide evidence of the commission of specified offenses, including, for example, murder, kidnaping, gambling, robbery, bribery, money laundering, terroristic threats, certain drug offenses, violations of the "Casino Control Act," endangering the welfare of a child and racketeering. This bill would expand the list to include health care fraud claims and fraudulent practices punishable by a term of imprisonment of more than one year.

3. While the act requires that any order to intercept begin and terminate as soon as practicable and that the interception be conducted in a manner which minimizes the interception of communication not otherwise subject to the court order, a law enforcement agency may be faced with the situation where the intercepted communication is in a language other than English or is in code. If this is the case and an interpreter or expert is not available during the interception period, the bill requires that the minimized interception be accomplished as soon as practicable. This requirement is consistent with federal law.

4. The bill provides that an order authorizing interception may be executed at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order. The bill defines "point of interception" as the site at which the investigative or law enforcement officer is located at the time the interception is made.

5. The act currently provides that a law enforcement officer who has obtained a warrant may require a provider of electronic communication service to disclose the contents of a communication without providing notice to the subscriber or the customer. The bill

includes remote computing service providers in this provision. The bill also requires a provider to disclose to a law enforcement agency, when the law enforcement entity obtains a grand jury or trial subpoena, information such as: the subscriber's name, address, telephone number or other number or identity, the length of service provided and the types of services utilized by the subscriber.

6. The act also currently requires that a provider disclose a record or other information pertaining to a subscriber or customer, other than the contents of a communication, provided the law enforcement agency obtains a warrant or consent from the subscriber or customer. The bill would authorize a third option: the provider would be required to disclose the information if the law enforcement agency obtained an order for disclosure. An order for disclosure may be issued by a judge only if the law enforcement agency offers specific and articulable facts showing reasonable grounds to believe that the record or other information pertaining to a subscriber or customer is relevant and material to an ongoing criminal investigation. The judge who issues such an order may quash or modify the order, on a motion by the service provider, if the information or records requested are unusually voluminous or compliance with such an order would cause an undue burden on the provider.

7. The bill provides that, upon request of a law enforcement agency, a provider shall take all necessary steps to preserve, for a period of 90 days, records and other evidence in its possession pending the issuance of a warrant. The preservation period shall be extended for an additional 90 days upon the request of the law enforcement agency.

8. The bill also implements a technical change for consistency with the federal law by omitting "wire" in reference to "provider of wire or electronic communication service" since wire communication service is included within the definition of electronic communication service. These changes are not intended to make any substantive changes to the act.

PO BOX 004
TRENTON, NJ 08625

Office of the Governor
NEWS RELEASE

CONTACT: Gene Herman

609-777-2600

RELEASE: June 30, 1999

Gov. Christie Whitman today signed the following pieces of legislation:

A-3014, sponsored by Assembly Members Joseph R. Malone, 3d, (R-Burlington/Monmouth /Ocean) and James W. Holzapfel (R-Monmouth/Ocean) and Senators Louis F. Kosco (R-Bergen) and John J. Matheussen (R-Camden/Gloucester), reauthorizes the New Jersey Wiretapping and Electronic Surveillance Act, which was due to expire on July 1, 1999. The Act allows law enforcement agencies to engage in electronic surveillance and wiretapping under certain conditions. The Act also governs other types of electronic surveillance, such as recordings made with the consent of one of the parties to the conversation, as well as interceptions of other electronically- transmitted information, including page messages, Internet communications and electronic-mail communications. The bill deletes the sunset provision.

A-2612, sponsored by Assembly Members Joseph V. Doria, Jr. (D- Hudson) and Joseph Charles, Jr. (D-Hudson) and Senator Edward T. O'Connor, Jr. (D-Hudson), repeals state law which authorized the designation of State Highway 440 to create a freeway through Bayonne. Plans to construct the roadway have been canceled as a result of strong local opposition to the roadway. The bill thus acts to delete what is essentially an obsolete reference in New Jersey law, and permit the area of the proposed route to be available for other purposes.