

Appendix A

State Wiretap Laws (as of June 1, 2002)

Overview

This survey of the law of each state regarding electronic communications focuses upon three substantive areas: (1) the use of wiretaps; (2) the use of pen register and trap-and-trace devices; and (3) the interception and retrieval of stored electronic communications. The initial heading provides, the state and statutory citations for the current law in each such area, which is summarized in the narrative section. The heading entitled “Party Consent” indicates the number of parties to a conversation, if any, who must consent before the communication may legally be intercepted and/or recorded. The final heading, “Legislation,” indicates whether pertinent legislation relating to electronic communications was introduced subsequent to the events of September 11 and has either been enacted or is still pending before the legislature of the state in question. If the response with regard to a particular state is “yes,” a summary of that legislation and its procedural status can be found in the companion survey entitled *State Wiretap Legislation, supra*, Appendix B.

The research for the survey was conducted by attorneys in the Washington, D.C., office of Morrison & Foerster LLP, in conjunction with the Constitution Project Initiative on Liberty and Security. The Constitution Project is a nonprofit bipartisan organization dedicated to achieving consensus on controversial issues. Its Liberty and Security Initiative is addressing a broad range of issues that have arisen since September 11, including the use of military tribunals, the detention of aliens and government security.

The research that provides the basis for this survey was limited to a review of pertinent statutory and other written materials. Representatives of the respective governments, law enforcement agencies, and legislatures of the various states were not consulted. Because of the limitations in the methodology used and the generality

of the survey, the information provided may not be applicable to all situations and should not be relied or acted upon without specific legal advice based upon the particular situation at issue. Moreover, because the survey reflects the state of the law as of June 1, 2002, the statutory requirements of a particular jurisdiction may have subsequently changed. For these reasons, the survey is not a substitute for professional advice based on specific issues.

This summary and possible updates are also available at <http://www.constitutionproject.org>, <http://www.mofo.com/practice>, and <http://www.peterswire.net>¹.

STATE: ALABAMA

ALA. CODE §§ 13A-11-30-37.

PARTY CONSENT: One**LEGISLATION: None****CURRENT LAW**

Alabama lacks a comprehensive statutory system regarding the interception of wire, oral and electronic communications.

STATE: ALASKA

ALASKA CODE §§ 2.20.300-.390; 12.37.010-.130 (Michie 2000).

PARTY CONSENT: One**LEGISLATION: None****CURRENT LAW****WIRETAP***Application:*

The Attorney General, or a person designated in writing or by law to act for the Attorney General, may authorize, in writing, an *ex parte* application to a court of competent jurisdiction for an order authorizing the interception of a private communication if the interception may provide evidence of, or may assist in the apprehension of persons who have committed, are committing, or are planning to commit, the following offenses: murder in the first or second degree, kidnapping, a class A or unclassified felony drug offense. (12.37.010).

A peace officer may intercept an oral communication by use of an electronic, mechanical, or other eavesdropping device that is concealed on or carried on the person of the peace officer and that transmits that oral communication by means of radio to a receiving unit that is monitored by other peace officers, if the interception and

1. The specific web pages may be directly accessed at the following: <http://www.peterswire.net/pssurv.html>, <http://www.mofo.com/practice/ArticleDetail.cfm?MCatID=&concentrationID=&ID=938&Type=3>, and http://www.constitutionproject.org/ls/Summary_State_Chart_2_WDF_v1.DOC.

April 2003]

STATE WIRETAP LAWS

989

monitoring occurs: during the investigation of a crime or the arrest of a person for a crime; and for the purpose of ensuring the safety of the peace officer conducting the investigation or making the arrest; the peace officer intercepting the conversation is a party to the oral communication and has consented to the interception; and the communication intercepted is not recorded. (12.37.400(a)).

Reports:

Within thirty days after the expiration of the authorized interception, the court entering the order shall report to the Administrative Office of the United States Courts the following information: the fact that there was application for order or extension, type applied for, whether it was granted or modified, the duration authorized, the offense specified in the order or extension, name of applicant and nature of place from which communications were intercepted. (12.37.130(a)).

In January of each year, the Attorney General or the Attorney General's designee shall report to the Administrative Office of the United States Courts the following information: the information with respect to each application for an order or extension order made; a general description of the interceptions made under the order or extension, including the nature, amount, and cost of the manpower involved in the interception; the number of arrests resulting from interceptions made under the order and the offenses for which arrests were made; the number of trials resulting from the interceptions; the number of motions to suppress made with respect to the interceptions, the number of such motions granted, and the number of such motions denied; and the number of convictions resulting from interceptions and the offenses for which the convictions were obtained, and a general assessment of the importance of the interceptions. (12.37.130(b)).

The Attorney General or the Attorney General's designee shall prepare and make available to the public annual reports containing the following information: number of applications made; number of orders entered by the court; effective period of time for which each interception was authorized; number of, and duration of the authorized interception period specified in, any extension orders; offenses in connection with which the communications were sought; names and titles of the applicants; number of indictments or other charges resulting from each application; offenses that each indictment or other charge relates to; and disposition of each indictment or other charge. (12.37.130(c)).

A person who is an employee of a communications common carrier or of an electronic communication service or of a private investigation agency, and has knowledge of the probable occurrence

political subdivision of Arizona to justify the officer's belief that an order should be issued; and (a) details as to the particular crime that has been, is being or is about to be committed; (b) identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) description of the type of communications sought to be intercepted; (d) description of the nature, identification and location of the communication facility from which or the place where the communication is to be intercepted. (13-3010(B)(1)-(2)).

The application shall also include: a full and complete statement as to whether other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; a statement of the period of time for which the interception is required to be maintained; a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each application. (13-3010(B)(3)-(5)).

If the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. (13-3010(B)(6)).

Order:

Upon proper application, a judge may enter an *ex parte* order authorizing interception, as requested or with any appropriate modifications. (13-3010(C)).

Each order authorizing the interception of any wire, electronic or oral communication shall specify all of the following: identity of the person, if known, whose communications are to be intercepted; nature and location of the communication facilities as to which or the place where authority to intercept is granted; particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates; identity of the agency authorized to intercept the communications and of the person authorizing the application; period of time during which the interception is authorized; that the authorization for interception be executed as soon as practicable, that it be conducted in such a way as to minimize the interception of communications not otherwise subject to interception and that it terminate upon attainment of the authorized objective or on the date specified, whichever comes first; and that entry may be made to service, install or remove interception devices or equipment if entry is necessary to effect the interception. (13-3010(D)).

An order may not authorize the interception of any wire or oral communication for any period that is longer than is necessary to achieve the objective of the authorization and that exceeds thirty days. This thirty-day period begins on the earlier of the day on which the interception actually begins under the order or ten days after the order is signed. The court may grant extensions but an extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and shall not exceed thirty days.

Emergency:

If the Attorney General or a county attorney or such prosecuting attorneys as they may designate in writing reasonably determines that an emergency situation exists involving immediate danger of death or serious physical injury to any person, and that such death or serious physical injury may be averted by interception of wire, electronic or oral communications before an order authorizing such interception can be obtained, the Attorney General or a county attorney or his designee may specially authorize a peace officer or law enforcement agency to intercept such wire, electronic or oral communications. (13-3015(A)).

The Attorney General or county attorney shall apply for an order authorizing the interception. The application shall be made as soon as practicable, and in no event later than forty-eight hours after commencement of the emergency interception. The application shall include an explanation and summary of any interception of communications occurring before the application for authorization. (13-3015(B)).

If the prosecuting attorney fails to obtain an authorization within forty-eight hours after commencement of the emergency interception, or if authorization to intercept communications is denied, the interception shall immediately terminate and any communications intercepted without judicial authorization may not be used as evidence in any criminal or civil proceeding against any person. (13-3015(C)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

Any prosecuting attorney or investigating peace officer of Arizona or its political subdivisions may apply to any justice of the supreme court, judge of the court of appeals, judge of the superior court or magistrate for an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device. The application shall be made in writing and under oath and shall state: name and

title of the applicant; telephone number or communication facility on which the pen register or trap and trace device is to be installed and the identity of the subscriber of the telephone number or communication facility; certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation; statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates. (13-3017(A)).

Order:

A judge shall issue an *ex parte* order authorizing the installation and use of a pen register or trap and trace device if the judge finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. An order shall specify: identity, if known, of the subscriber of the communication service or telephone line to which the pen register or trap and trace device is to be attached; number and, if known, physical location of the communication facility or telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits, if any, of the trap and trace order; statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; that, on the request of the applicant, the communication service provider shall furnish information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device and to identify subscribers of any communication facility or telephone number obtained by operation of such device. (13-3017(B)).

Extension:

An order authorizes the installation and use of a pen register or trap and trace device for a period of not to exceed sixty days. Extensions of the order may be granted, but only upon an application and judicial finding and shall not exceed sixty days. (13-3017(C)).

STORED ELECTRONIC COMMUNICATIONS:

An agency or political subdivision of this state may require the disclosure by a communication service provider or remote computing service of the contents of an oral, wire or electronic communication that has been in electronic storage for 180 days or less in one of the following ways:

1. Without prior notice to the subscriber or party, by obtaining a search warrant.

2. With prior notice to the subscriber or party, by serving a subpoena.

3. With prior notice to the subscriber or party, by obtaining a court order on an application and certification that contains specific and articulable facts showing that there are reasonable grounds to believe that the communication content sought is relevant to an ongoing criminal investigation. (13-3016(B)).

The notice to the subscriber or party may be delayed for a period of not to exceed ninety days under any of the following circumstances:

1. If the applicant for a search warrant or court order requests a delay of notification and the court finds that delay is necessary to protect the safety of any person or to prevent flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation.

2. If the investigator or prosecuting attorney proceeding by subpoena executes a written certification that there is reason to believe that notice to the subscriber or party may result in danger to the safety of any person, flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation. The agency shall retain a true copy of the certification with the subpoena. (13-3016(D)).

If further delay of notification is necessary, extensions of up to ninety days each may be obtained by application to the court. (13-3016(F)).

Any agency may apply for a court order directing the communication service provider or remote computing service not to notify any other person of the existence of the subpoena, court order or warrant for such period as the court deems appropriate. The court shall grant the application if it finds that there is reason to believe that notice may cause an adverse result.

STATE: ARKANSAS

PARTY CONSENT: One

ARK. CODE ANN. §§ 5-60-120, 5-16-101 (Michie 1997).

LEGISLATION: None

CURRENT LAW

Arkansas lacks a comprehensive statutory system regarding the interception of wire, oral and electronic communications.

April 2003]

STATE WIRETAP LAWS

995

STATE: CALIFORNIA **PARTY CONSENT:** All
CAL. PENAL CODE §§ 629.50–.98 **LEGISLATION:** Yes
(Deering 2002)

CURRENT LAW

WIRETAP:

Application:

Each application for an order authorizing the interception of a wire, electronic digital pager, or electronic cellular telephone communication shall be made in writing upon the personal oath or affirmation of the Attorney General, Chief Deputy Attorney General, or Chief Assistant Attorney General, Criminal Law Division, or of a district attorney, to the presiding judge of the superior court or one other judge designated by the presiding judge. Each application shall include all of the following information: identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; identity of the law enforcement agency that is to execute the order; statement attesting to a review of the application and the circumstances in support thereof by the chief executive officer, or his or her designee, of the law enforcement agency making the application; full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued; duration authorized, and if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of the facts establishing probable cause to believe that additional communications of the same type will occur thereafter; full and complete statement of the facts concerning all previous applications known, to the individual authorizing and to the individual making the application, to have been made to any judge of a state or federal court for authorization to intercept wire, electronic digital pager, or electronic cellular telephone communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each of those applications. (629.50(a)(1)–(6)).

Extension:

If the application is for the extension of an order, a statement setting forth the number of communications intercepted pursuant to the original order, and the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain results. (629.50(a)(7)).

The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. (629.50(b)).

Order:

A judge may enter an *ex parte* order, as requested or modified, authorizing interception of wire, electronic digital pager, or electronic cellular telephone communications initially intercepted within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following (this provision is operative until 1/08): there is probable cause to believe that: an individual is committing, has committed, or is about to commit, one of the following offenses: importation, possession for sale, transportation, manufacture, or sale of controlled substances where the substance exceeds ten gallons by liquid volume or three pounds of solid substance by weight; murder, solicitation to commit murder, the commission of a crime involving the bombing of public or private property, or aggravated kidnapping, and conspiracy to commit any of the above-mentioned crimes; particular communications concerning the illegal activities will be obtained through that interception, including, but not limited to, communications that may be utilized for locating or rescuing a kidnap victim; the facilities from which, or the place where, the wire, electronic digital pager, or electronic cellular telephone communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by the person whose communications are to be intercepted; normal investigative procedures have been tried and have failed or reasonably appear either to be unlikely to succeed if tried or to be too dangerous. (629.52).

PEN REGISTER/TRAP & TRACE DEVICE:

A magistrate may authorize installation of pen a register by issuance of search warrant. This is not codified in the California Penal Code but is contained in an Attorney General's opinion. *See* 69 Op. Cal. Att'y Gen 55. (1986).

April 2003]

STATE WIRETAP LAWS

997

STATE: COLORADO **PARTY CONSENT:** One
COLO. REV. STAT. §§ 18-9-301 **LEGISLATION:** Yes
to -313, 16-15-101 to -104 (1998)

CURRENT LAW

WIRETAP:

Application:

An *ex parte* order authorizing or approving the interception of any wire, oral, or electronic communication may be issued by any judge of competent jurisdiction of the state of Colorado upon application of the Attorney General or a district attorney, showing by affidavit that there is probable cause to believe that evidence will be obtained of the commission of any one of the following crimes or that one of these crimes will be committed: murder in the first or second degree; kidnapping in the first or second degree; professional gambling; robbery, aggravated robbery, or burglary in the first or second degree; bribery, compensation for past official behavior, attempt to influence a public servant, designation of supplier, or misuse of official information; dealing in controlled substances; crimes dangerous to life, limb, or property, meaning extortion, as defined as menacing by use of a deadly weapon, theft by means other than the use of force, threat, or intimidation, arson, and assault in the first or second degree; escape or introducing contraband in the first or second degree; criminal conspiracy to commit any of the aforementioned enumerated crimes; and limited gaming. (16-15-102(1)(a)).

An *ex parte* order for wiretapping or eavesdropping may be issued only for a crime for which a felony penalty is authorized upon conviction. (16-15-102(1)(b)).

Each application for an order authorizing or approving the interception of any wire, oral, or electronic communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information: identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including: details as to the particular offense that has been, is being, or is about to be committed, a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted; a particular description of the type of communication sought to be intercepted; and the identity of the person, if known,

committing the offense and whose communications are to be intercepted; complete statement as to whether other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried, or to be too dangerous; statement of the period of time for which the interception is required to be maintained; if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, there shall be required a particular description of the facts establishing probable cause to believe that additional communications of the same type will occur thereafter; complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application. (16-15-102)(2)(a)-(e)).

Extension:

If the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain those results. (16-15-102)(2)(f)).

The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. (16-15-102(3)).

Order:

Upon an application, the judge may enter an *ex parte* order, as requested or as modified, authorizing or approving the interception of any wire, oral, or electronic communication within the territorial jurisdiction of the court in which the judge is sitting and outside that jurisdiction but within the United States in the case of a mobile interception device, if the judge determines on the basis of the facts submitted by the applicant that there is probable cause for belief that: a person is committing, has committed, or is about to commit a particular offense enumerated above; particular communications concerning that offense will be obtained through the interception; normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or to be too dangerous; the facilities from which or the place where the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of an offense or are leased to, listed in the name of, or commonly used by the

person alleged to be involved in the commission of the offense. (16-15-102(4)).

Each order authorizing or approving wiretapping or eavesdropping shall specify: identity of the person, if known, whose communications are to be intercepted; nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; identity of the agency authorized to intercept the communications, and of the person authorizing the application; and period of time during which an interception is authorized, including a statement as to whether or not the interception automatically terminates when the described communication is first obtained. (16-15-102(5)).

No order may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization nor in any event longer than thirty days. Such thirty-day period begins the first day on which the investigative or law enforcement officer begins to conduct an interception under the order or ten days after the order is entered, whichever occurs earlier. (16-15-102(6)).

Extension:

An extension of an order may be granted but only upon application. The period of the extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception, and must terminate upon attainment of the authorized objective, or in any event in thirty days. No more than one extension may be granted for any order. In the event that the intercepted communication is in a code or foreign language and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception may be conducted in whole or in part by government personnel or by an individual operating pursuant to a contract with the government and acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. (16-15-102(6)).

Reports:

An *ex parte* order may require reports to be made to the judge who issued the order, showing what progress has been made toward

achievement of the authorized objective and the need for continued interception. Such report shall be made at such times as the judge may require. (16-15-102(7)).

All courts having jurisdiction to issue orders shall submit to the state court administrator reports, as prescribed by the chief justice of the supreme court of Colorado, on the number of applications for orders permitting wiretapping or eavesdropping, whether the applications were granted or denied, the period for which an interception was authorized, and whether any extensions were granted on the original order. (16-15-104(1)).

District attorneys shall report annually to the Attorney General information as to the number of applications made for orders permitting the interception of wire, oral, or electronic communications; the offense specified in the order or application; the nature of the facilities from which, or the place where, communications were to be intercepted; a general description of the interceptions made under any order or extension, including the nature and frequency of incriminating communications intercepted, the nature and frequency of other communications intercepted, the number of persons whose communications were intercepted, and the nature, amount, and cost of the manpower and other resources used in the interceptions; the number of arrests resulting from interceptions made under such order or extension and the offenses for which arrests were made; the number of motions to suppress made with respect to such interceptions and the number granted or denied; the number of convictions resulting from the interceptions and the offenses for which the convictions were obtained; and a general assessment of the importance of the interceptions. These reports shall be submitted to the Attorney General by February 1 of each year and shall include all orders and applications made during the preceding year. (16-15-104(3)).

Within a reasonable time, but not later than ninety days after the filing of an application for an order of approval, which application is denied, or after the termination of the period of an order or extensions thereof, the judge to whom the application was presented shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion is in the interest of justice, notice of the following:

1. The fact of the entry of the order or application;
2. The date of the entry and the period of authorized, approved, or disapproved interception, or the denial of the application; and
3. The fact that during the period wire, oral, or electronic communications were or were not intercepted. The judge, upon the filing of a motion, may, in his discretion, make available to any such

April 2003]

STATE WIRETAP LAWS

1001

person or his counsel for inspection such portions of the intercepted communications, applications, and orders as the judge determines to be in the interest of justice. On an *ex parte* showing of good cause to a judge of competent jurisdiction, the serving of the matter may be postponed. (16-15-102(8)(d)).

Emergency:

Any investigative or law enforcement officer specifically designated by the Attorney General or a district attorney may intercept wire, oral, or electronic communications for a period not to exceed twenty-four hours under the following circumstances: When an emergency situation exists that involves the holding of hostages or kidnapping by the use of physical force, a deadly weapon, or an explosive device, and there is imminent danger of serious bodily injury or death to any person and there are reasonable and sufficient grounds present upon which an order could be entered to authorize such interception. Any emergency interception shall terminate upon attainment of the authorized objective or at the end of the twenty-four-hour period, whichever comes first. (16-15-102(18)(a)-(b)).

PEN REGISTER/TRAP & TRACE DEVICE:

It shall not be unlawful: to use a pen register or a trap and trace device; or for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service from fraudulent, unlawful, or abusive use of such service. (18-9-305(4.5)).

STORED ELECTRONIC COMMUNICATIONS:

The Colorado statutes define electronic storage as:

1. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
2. Any storage of such communication by an electronic communication service for purposes of backup protection of such communication. (16-15-101(4.5)).

However, there is no section in the Col. Revised Statutes specifically addressing the access to and disclosure or use of stored oral, wire, and electronic communications.

STATE: CONNECTICUT **PARTY CONSENT:** One
CONN. GEN. STAT. §§ 53a-187 to **LEGISLATION:** Yes
-189, 54-41a to -41u (2001)

CURRENT LAW

WIRETAP:

Application:

The Chief State's Attorney or the state's attorney for the judicial district in which the interception is to be conducted may make application to a panel of judges for an order authorizing the interception of any wire communication by investigative officers having responsibility for the investigation of offenses as to which the application is made when such interception may provide evidence of the commission of offenses involving gambling, bribery, or felonious crimes of violence. (54-41b).

Each application for an order authorizing the interception of a wire communication shall be made in writing upon oath or affirmation to a panel of judges. Each application shall include the following information: 1) identity of the applicant and his authority to make such application; 2) identity and qualifications of the investigative officers or agency for whom the authority to intercept a wire communication is sought; 3) identity and qualifications of the investigative or law enforcement officers to whom disclosure of the contents of any intercepted wire communication or evidence derived therefrom might be made; 4) statement of the use to which the contents of any intercepted wire communication or any evidence derived therefrom will be put. (54-41c).

The application shall also contain: 5) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his reasonable belief that the wire communication of a particularly described person will constitute evidence of a crime that has been or is being committed or that such communication will materially aid in the apprehension of the perpetrator of such crime and that an order should be issued, including (a) details as to the particular offense that has been or is being committed, (b) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (c) a particular description of the type of communications sought to be intercepted, (d) the identity of the person, if known, who has committed or is committing the offense and whose communications are to be intercepted, (e) the time and date when the facts and circumstances relied upon by the applicant were first received by him or by the investigative or law enforcement officer conducting the

investigation, whichever is earlier, (f) the way in which the intercepted wire communication will constitute material evidence of the particularly described offense or will materially aid in the apprehension of the perpetrator of such offense, (g) the hours of the day or night during which wire communication may be reasonably expected to occur; 6) a full and complete statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ; 7) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; 8) a full and complete statement of the facts concerning all previous applications known to the individual making the application, made to any panel of judges, for authorization to intercept, or for approval of interceptions of, wire communications involving any of the same persons, facilities or places specified in the application, and the action taken by the panel on each such application; 9) a statement that the wire communications sought are material to a particularly described investigation or prosecution and that such communications are not legally privileged; 10) if it is reasonably necessary to make a secret entry upon a private place or premises in order to install an intercepting device to effectuate the interception, a statement to that effect and to the effect that no practicable alternative method of executing the order which will preserve the secrecy of its execution exists; 11) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results; 12) where the application is for an order authorizing interception in excess of thirty-five orders previously issued by all panels in a calendar year, a statement setting forth the nature of the emergency situation which may result in imminent peril to the public health, safety or welfare, and the nature of that imminent peril, which requires the issuance of an additional interception order; 13) such additional testimony or documentary evidence in support of fact in the application as the panel of judges may require. (54-41c).

Order:

A panel of judges, by unanimous vote, may enter an *ex parte* order authorizing the interception of wire communications within the state of Connecticut, if the panel determines on the basis of the facts submitted by the applicant that there is probable cause to believe

that: an individual has committed or is committing one of the offenses enumerated above; particular communications will constitute material evidence that an offense enumerated above has been committed or is being committed or will materially aid in the apprehension of the perpetrator of such offense; such communications are not otherwise privileged; other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ; the facilities from which, or the place where, the wire communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such individual; such facilities or places are not those exempt by statute; if the facilities from which a wire communication is to be intercepted are public, a special need exists to intercept wire communications over such facilities; the investigative officers to be authorized to intercept the wire communication are qualified by training and experience to execute the interception sought; not more than thirty-four orders authorizing interception have been previously issued by all panels in the calendar year in which the application is made, except that upon a showing of an emergency situation in which the commission of an offense may result in imminent peril to public health, safety or welfare, such panel may issue additional orders authorizing interception. (54-41d).

Each order authorizing the interception of any wire communication shall be accompanied by a written statement of the panel setting forth in detail its determination and the grounds therefor and shall specify: identity of the person, if known, whose communications are to be intercepted; nature and location of the communication facilities as to which or the place where authority to intercept is granted; particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; identity of the investigative officers authorized to intercept such wire communications; identity of the investigative or law enforcement officers to whom disclosure of the contents of any intercepted wire communication or any evidence derived therefrom may be made; use to which the contents of any intercepted wire communication or any evidence derived therefrom may be put; identity of the person making the application and his authority; identity of the panel and its authority to issue an order; period of time during which such interception is authorized, including a statement that the interception shall automatically terminate when the desired communication has been first obtained; express authorization to make secret entry onto private premises to install any device, provided no such secret entry shall be authorized if there

April 2003]

STATE WIRETAP LAWS

1005

exists a practicable alternative method of executing the order which will preserve the secrecy of its execution; date of issuance of the order and its effective date. (54-41e).

Extension:

Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception, and shall terminate upon attainment of the authorized objective, or in any event within fifteen days next succeeding the date of issuance of such order. An order authorizing the interception of a wire communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant at the prevailing rates. (54-41e).

An order may be executed according to its terms only during the hours specified therein, and for the period authorized or part thereof. No order may authorize the interception of any wire communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than fifteen days. (54-41f).

No more than three extensions of an order may be granted by the panel and only upon application for an extension. (54-41g).

If the facilities from which, or the place where, the wire communications are to be intercepted are being used, or are about to be used, or are leased to, listed in the name of, or commonly used by, a licensed physician, an attorney-at-law or a practicing clergyman, no order shall be issued and no wire communications shall be intercepted over such facilities or in such places. (54-41h).

Reports:

Whenever an order authorizing an interception is entered, the order may require reports to be made to the panel showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as such panel may require. (54-41f).

In addition to any reports required by federal law, within thirty days next succeeding the expiration of an order or an extension thereof, or the denial of an application, the panel shall report to the

Chief Court Administrator the fact that an order or extension was applied for; the fact that the order or extension was granted as applied for, was modified or was denied; the period of interceptions authorized by the order, and the number and duration of any extensions of the order; the offense or offenses specified in the order or application, or extension of an order; the identity of the person making the application and the nature of the facilities from which or the place where communications were to be intercepted. (54-41n). In January of each year, each state's attorney shall report to the Administrative Office of the United States courts and to the Chief Court Administrator, who shall in turn report to the Governor and the General Assembly, the information required with respect to each application for an order or extension made during the preceding calendar year. (54-41o).

PEN REGISTER/TRAP & TRACE DEVICE:

The requirements to obtain an *ex parte* order for a pen register or trap and trace device are less stringent. An application may be made by the Chief State's Attorney, a deputy chief state's attorney, a state's attorney, or an assistant state's attorney to the superior court. No panel of judges or unanimous consent required. The application requires (1) the identity of the applicant, and (2) a certification by the applicant of the information likely to be obtained. An *ex parte* order for a pen register or trap and trace device is good for a period of sixty days. Also, a law enforcement officer, under the direction of any of the parties eligible to make an application, may initiate pen register or trap and trace device interception in an emergency situation as long as an application is made within forty-eight hours of initiating such activities. Finally, a state's attorney or the chief law enforcement officer for a town may issue a subpoena to require a telecommunications service provider to disclose records pertaining to a subscriber or a customer if either applicant reasonably believes such information is relevant to an ongoing criminal investigation.

April 2003]

STATE WIRETAP LAWS

1007

STATE: DELAWARE
DEL. CONST. art. I, § 6; DEL.
CODE ANN. tit. 11 §§ 1335; 2401–
34 (1999)

PARTY CONSENT: One
(Violations of Privacy—All)

LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Application:

An application for an interceptive order may be made by the Attorney General, chief deputy Attorney General, state prosecutor or chief prosecutor of any county to a court authorized to receive an application to commence interception. (11 § 2405).

An application for an *ex parte* order shall be made in writing upon oath or affirmation to a judge of competent jurisdiction. A judge is defined as one or more of the several Judges of the Superior Court to be designated from time to time by the President Judge of the Superior Court to receive applications for and to enter orders authorizing interception of wire, oral or electronic communications pursuant to this statute. The application shall provide the following information: (1) identity of the investigative or law enforcement officer and the officer authorizing the application; (2) complete statement of facts and circumstances including (a) details of the particular offense that has been committed, is being committed or will be committed; (b) the nature and location of the communication facilities; (c) a description of the type of communication sought; and (d) the identity of the person who committed or is about to commit the offense and whose communications are to be intercepted; and (3) statement as to whether other investigative procedures have been tried and failed or whether other investigative procedures will unlikely succeed or are too dangerous. The application should also provide a description of previous applications made to any judge involving the same persons, facilities or places and the action taken by the judge, and the time period for which interception is sought. A judge may request additional testimony or documentary evidence in support of an application. (11 § 2407(a)–(b)).

The application must be made in connection with the offenses of racketeering, murder, kidnapping, gambling, robbery, bribery, extortion, dealing in narcotic drugs or dangerous drugs, dealing in central nervous system depressant or stimulant drugs, dealing in controlled substances or counterfeit controlled substances, prison escape, jury tampering, or stalking. In addition, an application may be made if it is a felony creating a risk of physical injury to any person

or it involves a conspiracy or solicitation to commit a crime listed above. (11 § 2405).

An interception may be conducted in whole or in part by federal, state or local government personnel, or by an individual operating under a contract with the state or a political subdivision of the state acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. (11 § 2407(e)(4)).

Order:

An *ex parte* order may authorize the interception of a wire, oral or electronic communication within the territorial jurisdiction of the court with which the application was filed. If an application for an *ex parte* order is made by the Attorney General or other designee, an order may authorize the interception of communications sent or received by a mobile telephone anywhere within the state so as to permit the interception of the communications regardless of whether the mobile telephone is physically located within the jurisdiction of the court in which the application was filed at the time of the interception; however, the application must allege that the offense being investigated may transpire in the jurisdiction of the court in which the application is filed. (11 § 2407(c)).

Each order authorizing the interception of any wire, oral or electronic communication shall specify: the identity of the person, if known, whose communications are to be intercepted; the nature and location of the communications facilities as to which or the place where authority to intercept is granted; a description of the type of communication sought to be intercepted and a statement of the offense to which it relates; the identity of the agency authorized to intercept the communications and of the person authorizing the application; and the period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (11 § 2407(d)(1)).

An *ex parte* order may be no longer than necessary but in any case no longer than thirty days. (11 § 2407(e)(1)).

Emergency:

In case of emergency situation that involves immediate danger of death or serious physical injury to any person, activities related to escape or attempted escape from custody, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime, interception activities may commence and an application for an *ex parte* order be made within 48 hours of commencing interception. If the application is denied, interception activities cease immediately. (11 § 2407(e)(5)).

April 2003]

STATE WIRETAP LAWS

1009

An application to extend an order must include all the information required in the original application, the judge must make the same findings and the application must include a statement setting forth the results obtained from the interception or a reasonable explanation of the failure to obtain the results. (11 § 2407(e)(2)).

Reports:

By judge: Within thirty days after the expiration of an order or an extension or renewal thereof entered under this statute or the denial of an order confirming verbal approval of interception, the issuing or denying Judge shall make a report to the President Judge of the Superior Court stating: that an order, extension or renewal for which application was made; the type of order for which application was made; that the order was granted as applied for, was modified or was denied; the period of the interceptions authorized by the order and the number and duration of any extensions or renewals of the order; the offense specified in the order or extension or renewal of an order; the identity of the person authorizing the application and of the investigative or law-enforcement officer and agency for whom it was made; and the character of the facilities from which or the place where the communications were to be intercepted. (11 § 2408(a)).

By Attorney General: The Attorney General or Deputy Attorney General specifically designated by the Attorney General shall make and file all reports required by federal law. (11 § 2408(b)).

To issuing judge: Whenever an order authorizing interception is entered, the order shall require reports to be made to the judge showing what progress has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at the time and place required by the issuing judge. (11 § 2407(f)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

An application to install a pen register or trap and trace device may be made by a law enforcement or investigative officer, and the application should provide the names of the officers, the identity of the law-enforcement agency conducting the investigation and a statement under oath that the information likely to be obtained is relevant to an ongoing criminal investigation conducted by that agency. (11 § 2432). The statute exempts electronic communication service providers who install such devices in the regular course of their business or who are cooperating with law enforcement officers

pursuant to an *ex parte* order. (11 § 2431). A court of competent jurisdiction means the Superior Court of the State. (11 § 2430).

Order:

An order issued shall:

1. specify the identity, if known, of the person to whom is leased or in whose name is listed the electronic communication service to which the pen register or trap and trace device is to be attached;

2. specify the identify, if known, of the person who is the subject of the criminal investigation;

3. specify the number and, if known, physical location of the electronic communication service to which the pen register or trap and trace device is to be attached and in the case of the trap and trace device, the geographic limits of the trap and trace order;

4. contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

5. direct, upon the request of the application, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. (11 § 2433(b)).

An *ex parte* order to install a pen register or trap and trace device is valid only for a period of sixty days. An order may be extended with an application containing all information required in original application and upon same judicial findings, and may not exceed sixty days. (11 § 2433(c)).

STORED ELECTRONIC COMMUNICATIONS:

Except as authorized under the wiretapping, electronic surveillance statute, a person may not obtain, alter or prevent authorized access to wire or electronic communication while it is in electronic storage in an electronic communication system. (11 § 2421(a)). A person or entity providing an electronic communication service or remote computing service to the public may not divulge to any other person or entity the contents of a communication while in electronic storage. (11 § 2422(a)).

An investigative or law-enforcement officer may require disclosure of electronic communication that is in electronic storage for 180 days or less only in accordance with a search warrant issued by a court of competent jurisdiction. (11 § 2423(a)).

An investigative or law-enforcement officer may require disclosure of electronic communication that is in electronic storage for over 180 days:

1. without prior notice to subscriber or customer, if the officer obtains a search warrant; or

April 2003]

STATE WIRETAP LAWS

1011

2. with prior notice to subscriber or customer if the officer obtains (a) a subpoena issued by a court of competent jurisdiction, a grand jury or as authorized under the State Department of Justice; or (b) a court order. (11 § 2423(b)).

JURISDICTION: DISTRICT OF COLUMBIA
D.C. CODE ANN. §§ 23-541 to-546 (1996)

PARTY CONSENT: One

LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The U.S. attorney for D.C. may authorize in writing any law enforcement or investigative officer to make an application for a court order to intercept oral or wire communications. The U.S. attorney may also authorize a law or investigative law enforcement officer to make an application for an order of approval of the previous interception when the contents of the communication involve (a) an offense not specified in the interceptive order, (b) an emergency situation, or (c) in an emergency situation of an offense not contemplated at the time interception was made. (23-546(a)-(b)).

An application for an order is appropriate if it involves the following offenses (or conspiracy to commit the following offenses): (a) arson; (b) burglary; (c) destruction of property in excess of \$200; (d) gambling; (e) kidnapping; (f) murder; (g) robbery; (h) threats as specified in Section 1501 of Omnibus Crime Control and Safe Streets Act of 1968; (i) bribery; (j) offenses involving the sale or manufacture of controlled substances; (k) extortion; (l) blackmail; (m) obstruction of justice; (n) receipt of stolen property worth over \$250; (o) theft of property worth over \$250; and (p) trafficking in stolen property. (23-546(c)).

An application for an order must be made in writing upon oath or affirmation to a judge and state the applicant's authority to make the application. The application must provide the following information: (a) identity of the investigative or law enforcement officer and the officer authorizing the application; (b) complete statement of facts and circumstances including (i) details of the particular offense that has been committed, is being committed or will be committed, (ii) the nature and location of the communication facilities, (iii) a description of the type of communication sought, and (iv) the identity of the person who committed or is about to commit

the offense and whose communications are to be intercepted; and (c) statement as to whether other investigative procedures have been tried and failed or whether other investigative procedures will unlikely succeed or are too dangerous. The application should also provide a description of previous applications made to any judge involving the same persons, facilities or places and the action taken by the judge, and the time period for which interception is sought. (23-547(a)).

Order:

A judge of the Superior Court of the District of Columbia, a judge of the District of Columbia Court of Appeals, a judge of the United States District Court for the District of Columbia, or a judge of the United States Court of Appeals for the District of Columbia circuit may issue an order. (23-541).

An order shall specify (a) the identity of the person whose communications are to be intercepted; (b) the nature and location of the communications facilities; (c) a description of the communications sought to be intercepted and the offense to which it relates; (d) the identity of the agency authorized to intercept the communications; and (e) the period of time that interception is authorized (including whether or not interception terminates when the described communication has been obtained). (23-547(e)).

An interception order is good as long as necessary but not longer than thirty days. Extensions are granted only upon application. An application to extend an order must include all the information required in the original application, the judge must make the same findings and the application must include a statement setting forth the results obtained from the interception or a reasonable explanation of the failure to obtain the results. The period of extension shall be no longer than necessary and in no event longer than thirty days. (23-547(g)).

Emergency:

Any investigation or law enforcement officer specially designated by the U.S. attorney for the District of Columbia, who reasonably determines that an emergency situation exists with respect to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order could be obtained and there are grounds upon which an order could be entered, may intercept the communication if an application is initiated within twelve hours and completed within seventy-two hours after the interception has occurred or begins to occur. If the officer intercepts communications relating to offenses other than in

April 2003]

STATE WIRETAP LAWS

1013

order, the officer must make application as soon as practicable. (23-548).

Reports:

Within thirty days of the expiration of an *ex parte* order or extension order or the denial of an order, the court shall report to the chief judge of the D.C. Court of Appeals that (1) an order or extension was applied for, (2) the kind of order or extension applied for, (3) whether the order or extension was granted, denied or modified, (4) the period of the interception order and the number and duration of any extensions thereof, (5) offense specified in the order or application, (6) the identity of the investigative or law enforcement officer, the agency making the application and person authorizing the application, and (7) the character and location of the facilities where interception occurred. (23-555(a)).

Every January, the U.S. attorney for D.C. shall report to the Congress of the U.S. and the chief judge of the D.C. Court of Appeals the information listed above. In addition, the report to Congress shall also contain a general description of the interceptions made under such order including, character and frequency of incriminating communications, the character and frequency of other communications, the number of persons whose communications were intercepted, amount of manpower expended for interception activities, the number of arrests made, the type of offenses, the number of trials, the number of motions to suppress made with respect to such interceptions, the number of motions to suppress granted or denied, the number of convictions, and a general assessment of the importance of the interception. The information should also contain a general comparison to previous years. Reports should be made in accordance with regulations prescribed by the Director of the Administration Office of the U.S. Courts under section 2519(3) of Title 18, U.S. Code. (23-555(b)-(c)).

Report to Issuing Judge. Whenever an order authorizing interception is entered, the order *may* require reports to be made to the judge showing what progress has been made and the need for continued interception. Reports shall be made at such intervals as the judge may require. (23-547(h)).

STATE: FLORIDA
FLA. CONST. art. 1, §§ 12, 23;
FLA. STAT. §§ 934.01–.43 (2001)

PARTY CONSENT : All (One, if
investigative or law enforcement
officer intercepts or is party to
conversation)

LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Application:

The governor, Attorney General, statewide prosecutor, or any state attorney may authorize a written application to intercept wire, oral, or electronic communications to a court of competent jurisdiction. Interception is allowed in connection with the crimes of murder, kidnapping, aircraft piracy, arson, gambling, robbery, burglary, theft, dealing in stolen property, criminal usury, bribery, extortion, or any conspiracy or solicitation to commit any of these enumerated crimes (that statute also cites to various other provisions that enumerate other crimes).

The Department of Law Enforcement or any law enforcement agency having responsibility for investigation of the above enumerated offenses may be authorized to intercept wire, oral or electronic communications. “Law enforcement agency” is defined as an agency of the State of Florida or a political subdivision thereof or of the United States if the primary responsibility of the agency is the prevention and detection of crime or the enforcement of the penal, traffic, or highway laws of Florida and if its agents and officers are empowered by law to conduct criminal investigations and to make arrests. (934.07(1), 934.02(10)).

The Department of Law Enforcement, together with other assisting personnel as authorized and requested by the department may be authorized to intercept a communication for the investigation of the offense as to which the application is made when such interception may provide or has provided evidence of the commission of any offense that may be an act of terrorism or in furtherance of an act of terrorism or evidence of any conspiracy or solicitation to commit any such violation. (934.07(1)).

In addition, an interception may be conducted by government personnel or by an individual operating under a contract with the government, acting under the supervision of an agent or officer of the law enforcement agency authorized to conduct the interception. (934.09(5)).

A judge of competent jurisdiction is defined as a “justice of the Supreme Court, judge of a district court of appeal, circuit judge, or

April 2003]

STATE WIRETAP LAWS

1015

judge of any court of record having felony jurisdiction of the State of Florida, irrespective of the geographic location or jurisdiction where the judge presides.” (934.02(8)).

The application must be made in writing, under oath or affirmation and state applicant’s authority to make such application. The application must provide (1) the identity of the investigative or law enforcement officer making the application and the officer authorizing the application, (2) the facts and circumstances relied upon justifying an approval of the application, (3) details of the particular offense that either has been, is being, or will be committed, (4) description of the nature and location of facilities from which the communications are to be intercepted (there are exceptions to this requirement), (5) description of type of communications, and (6) identity of the person, if known committing the offense and whose communications are to be intercepted. The application must also include a statement as to whether other investigative procedures have been tried or reasonably appear likely not to succeed or are too dangerous, a time period for conducting interception activities, a complete statement of facts concerning all previous applications made to any judge involving any of the same persons, facilities, or places specified in the application and the actions taken by the judge. (934.09(1)).

Order:

The judge may issue an *ex parte* order authorizing the interception within the territorial jurisdiction of the court in which the judge is sitting and outside such jurisdiction but within the State of Florida in the case of a mobile interception device authorized by the judge within such jurisdiction, if the judge finds that:

there is probable cause that an individual is committing, has committed, or is about to commit a particular enumerated offense;

there is probable cause that particular communications will be obtained through the interception;

normal investigative procedures have been tried (or unlikely to succeed if tried or are too dangerous); and

there is probable cause that the facilities from where interception will occur (subject to certain exceptions) is being used or about to be used to commit a crime or are leased to, listed in the name of, or commonly used by such person. (934.09(3)).

Each order authorizing or approving the interception of any wire, oral, or electronic communication shall specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) a particular description of the type of communication sought to be

intercepted and a statement of the particular offense to which it relates; (d) the identity of the agency authorized to intercept the communications and of the person authorizing the application; and (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (934.09(4)).

The interception order is valid until the objective has been achieved but in no event longer than thirty days. Such thirty-day period begins on the day on which the agent or officer of the law enforcement agency first begins to conduct an interception under the order or ten days after the order is entered, which occurs earlier. (934.09(5)).

An application to extend an order must include all the information required in the original application, the judge must make the same findings and the application must include a statement setting forth the results obtained from the interception or a reasonable explanation of the failure to obtain the results. (934.09(5)).

Emergency:

In emergency cases, any investigative or law enforcement officer specially designated by the governor, Attorney General, the statewide prosecutor, or a state attorney, where there immediate danger of death or serious physical injury, the danger of escape of a prisoner, or conspiratorial activities threatening the security interest of the nation or state and requires that a wire, oral or electronic communication be intercepted before an order may be obtained, may authorize such interception. In addition, there must be grounds upon which an interception or order could be granted and an application must be made within 48 hours of starting the interception activity. (934.09(7)).

Reports:

To Issuing Judge: whenever an order authorizing interception is entered, the order *may* require reports to be made to the judge showing what progress has been made toward the achievement of the authorized objective and the need for continued interception. Reports shall be made at such intervals as the judge may require. (934.09(6)).

PEN REGISTER/TRAP & TRACE DEVICE:

The governor, Attorney General, a state attorney, the statewide prosecutor, a designated assistant state attorney, or assistant statewide prosecutor may make an application for an order

April 2003]

STATE WIRETAP LAWS

1017

authorizing or approving the installation and use of a pen register or trap and trace device, in writing under oath or equivalent affirmation, to the judge of competent jurisdiction. The application must include the identity of the applicant, the identity of the law enforcement agency conducting the investigation and a certification of the information likely to be obtained. (934.32).

The court shall enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court. The order must specify:

the identity, if known, of the person to whom is leased or in whose name is listed on the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

the identity, if known, of the person subject to the criminal investigation;

the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location and geographic limits; and

a statement of the offense to which the information is likely to be obtained.

The order is good for a period of sixty days. (934.33).

Emergency:

Emergency must involve immediate danger of death or serious physical injury or escape of prisoner and requires installation of pen register or a trap and trace device before an order authorizing such installation can be obtained, and there are grounds upon which an order could be entered. Must obtain an order within forty-eight hours after installation has occurred. (934.31(4)).

An order can be extended for another sixty-day period upon application with all information required in the original application and the judge must make the same findings. Extension may not exceed sixty days. (934.33(3)).

STORED ELECTRONIC COMMUNICATIONS:

Statute prohibits accessing a facility through which an electronic communication service is provided or exceeding authorization to access and thereby obtains electronic communication while it is in electronic storage. (934.21(1)).

An investigative or law enforcement officer may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for 180 days or less only pursuant to a warrant issued by the judge of a court of competent jurisdiction. An investigative or law enforcement officer may require the disclosure by a provider of electronic

communication services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than 180 days by requiring a provider of remote computing service to disclose the contents of any wire or electronic communication either: (a) without notice to the subscriber if officer obtains a warrant; (b) with prior notice, or with deferred notice (up to ninety days) by issuing court upon showing immediate notice would have adverse impact, from the officer to the subscriber if the investigative or law enforcement officer: (1) uses a subpoena; or (2) obtains a court order for such disclosure. (934.23(2)).

An investigative or law enforcement officer may require disclosure of any electronic communication that is held or maintained on a remote computing service: (a) on behalf of a subscriber or customer of such service and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of such service; (b) solely for the purpose of providing storage or computer processing services to a subscriber or customer, if the provider is not authorized to access the contents of any such communication for purposes of providing any service other than storage or computer processing. (934.23(3)).

An investigative or law enforcement officer may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication, only when the investigative or law enforcement officer obtains a warrant, obtains a court order, has the consent of the subscriber or customer or seeks certain information specified in the statute. (934.23(4)).

STATE: GEORGIA
GA. CONST. art. 1, § 1; GA.
CODE. ANN. §§ 16-11-60 to -69
(2001)

PARTY CONSENT: One
LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Application:

The district attorney having jurisdiction over the prosecution of crime under investigation or the Attorney General, may apply, in writing and under oath, for a warrant permitting the use of a device for the surveillance of such person or place.

April 2003]

STATE WIRETAP LAWS

1019

The application must contain the basis for the probable cause that a person is committing or has committed any of the enumerated crimes or that a private place is being utilized or has been utilized for the commission of any of the enumerated crimes and a description of the person or place, the crime or crimes, the device or devices to be used, and the specific conversations and activities to be overheard or observed. (16-11-64(c)).

Order:

Investigation warrants shall be valid for no more than twenty days after issuance, unless renewed for additional twenty-day periods for good cause shown at the time of written application for each such renewal. An interception may be conducted in whole or in part by law enforcement personnel or by an individual operating under a contract with a law enforcement agency and acting under the supervision of a law enforcement officer authorized to conduct the interception. (16-11-64(c)).

Any judge of the superior court having jurisdiction of such enumerated crimes may issue an investigation warrant permitting the use of a device as defined above for the surveillance of such person or place. The warrant must specify the purpose, duration, and circumstances of use permitted, the crime or crimes allegedly being committed, and the person or persons and place or places to be subject to surveillance. (16-11-64(c)).

Emergency:

If the Attorney General or a district attorney of the judicial circuit having jurisdiction over the emergency situation described herein or where the observation, monitoring, or recording of the activities of any person may occur, as provided in this subsection, determines that:

an emergency situation exists involving the immediate danger of death or serious physical injury to any person;

the emergency situation requires the immediate interception of a wire, oral, or electronic communication or the immediate observation, monitoring, or recording of the activities of any person involved in the emergency situation before an order authorizing such interception or surveillance can be obtained; and

there are grounds upon which an investigation warrant could be issued,

then any investigative or law enforcement officer specifically designated by the prosecuting official making such determination may utilize any device to intercept the communication or to observe, monitor, or record the activities of the person or persons involved in the emergency situation. An application must be made within forty-

eight hours after the interception or surveillance commences. Interception or surveillance may continue only so long as the emergency exists. (16-11-64.3).

Reports:

The officer executing the order to intercept wire, oral and electronic communications must make a "return" of the warrant to the judge describing how the warrant was used and what was obtained as a result. The return shall state with particularity the law enforcement officer or officers or their agents who actually employed the devices used in the execution of the warrant. The applicant for the warrant shall return same and report back to the judge issuing same within thirty days of the issuance of the warrant. In the event no evidence of one of the specific crimes set forth in the statute has been obtained through the use of such device or devices, it shall be the duty of the applicant physically to destroy all evidence obtained by surveillance and to certify that fact in writing to the judge under oath.

PEN REGISTER/TRAP & TRACE DEVICE:

Any district attorney or the Attorney General is authorized to make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device to a superior court for the circuit wherein the pen register or trap and trace device is to be installed and used, and the superior court for that circuit is authorized to enter an order authorizing the use of a pen register or a trap and trace device, to the extent the same is consistent with and permitted by the laws of the United States. (16-11-64.1).

Emergency must involve immediate danger of death or serious bodily injury to any person or conspiratorial activities characteristic of organized crime that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can be obtained. There also must be grounds upon which an order could be entered under the laws of the US to authorize such installation and use. Within forty-eight hours of installation must obtain order approving the installation of such.

April 2003]

STATE WIRETAP LAWS

1021

STATE: HAWAII
HAW. CONST. art. I, §§ 6-7;
HAW. REV. STAT. §§ 711-1111,
803-41 to -47 (2001)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The Attorney General, a designated deputy Attorney General in the Attorney General's absence or incapacity, or the prosecuting attorney of each county or a designated deputy prosecuting attorney in the prosecuting attorney's absence or incapacity, may make an application to a circuit court judge designated by the chief justice of the Hawaii supreme court or any other circuit court judge or district court judge, if a circuit court judge has not been so designated, or is otherwise unavailable, in the county where the interception is to take place, for an order authorizing or approving the interception of wire, oral or electronic communications. (803-44).

Each application for an order authorizing or approving the interception or a wire, oral, or electronic communication shall be made in writing upon oath or affirmation and shall include:

the identity of the investigative or law enforcement officer(s) requesting the application, the official(s) applying for an order;

a full and complete statement of the facts and circumstances relied upon by the applicant, to justify the applicant's belief that an order should be issued, including (a) details as to the particular offense that has been, is being, or is about to be committed, (b) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (c) a particular description of the type of communications sought to be intercepted, (d) the identity or descriptions of all persons, if known, committing the offense and whose communications are to be intercepted, and where appropriate (e) the involvement of organized crime;

a full and complete statement of the facts concerning how the interception is to be accomplished, and if physical entry upon private premises is necessary, facts supporting such necessity;

a full and complete statement of facts as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

a statement of facts indicating the period of time for which the interception is required to be maintained. If the nature of the

investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any court for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the court on each such application; and

where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. (803-46(a)).

Order:

Court may grant an interception order when such interception may provide or has provided evidence of murder, kidnapping, felony property damage, organized crime, extortion, bribery of a juror, witness or police officer, receiving stolen property, gambling, distribution of dangerous, harmful or detrimental drugs. (803-44)

Each order authorizing or approving the interception, of any wire, oral, or electronic communication shall specify: (1) the identity or description of all persons, if known, whose communications are to be intercepted; (2) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and the means by which such interceptions shall be made; (3) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (4) the identity of the agency authorized to intercept the communications and the persons applying for the application; (5) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained; and (6) how the authorization is to be accomplished. (803-46(d)).

No order shall authorize the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. The thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension which must include all the information in

the original application and the judge must make the same findings. The period of extension shall be no longer than the authorizing circuit court deems necessary to achieve the purposes of which it was granted and in no event longer than fifteen days. (803-46(e)).

Reports:

Whenever an order authorizing interception is entered, the order shall require reports to be made to the court which issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the court may require. (803-46(f)).

In January of each year, the Attorney General and county prosecuting attorneys must report to the administrative director of the courts and to the Administrative Office of the United States Court: (a) the fact that an order or extension was applied for; (b) the kind of order or extension applied for; (c) the fact that the order or extension was granted as applied for, was modified, or was denied; (d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (e) the offense specified in the order or application, or extension of an order; (f) the identity of the investigative or law enforcement officer and agency requesting the application and the person authorizing the request for application; (g) the nature of the facilities from which or the place where communications were to be intercepted; (h) a general description of the interceptions made under such order or extension, including (1) the approximate nature and frequency of incriminating communications intercepted; (2) the approximate nature and frequency of other communications intercepted, (3) the approximate number of persons whose communications were intercepted, and (4) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions; (i) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made; (j) the number of trials resulting from such interceptions; (k) the number of motions to suppress made with respect to such interceptions, and the number granted or denied; (l) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; (m) the information required by items (b) through (f) above with respect to orders or extensions obtained in a preceding calendar year and not yet reported; and (n) other information required by the rules and regulations of the Administrative Office of the United States Courts. (803-47(a)).

In March of each year, the administrative director of the courts shall transmit to the legislature a full and complete report concerning the number of applications for orders authorizing the interceptions of wire, oral, or electronic communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the administrative director of the courts by the Attorney General and prosecuting attorneys. (803-47(b)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

Upon application for an order authorizing the installation and use of a pen register or a trap and trace device, the reviewing judge shall satisfy himself or herself that there are sufficient facts and circumstances contained within the application that there is probable cause to believe that information will be obtained through the installation and use of a pen register or a trap and trace device which will constitute the fruits, instrumentalities, or evidence of a crime or is relevant to an ongoing criminal investigation. If the reviewing judge is so satisfied, the order issued shall specify: (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (b) the identity, if known, of the person who is the subject of the criminal investigation; (c) the number and, if known, the physical location of the telephone line to which the pen register or the trap and trace device is to be attached, and, in the case of a trap and trace device, the geographical limits of the trap and trace order; (d) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and (e) upon the request of the applicant, the information, facilities, and technical assistance necessary to accomplish installation of the pen register or trap and trace device that the provider of wire communication service is directed to furnish to the applicant. (803-44.6(a)-(b))

The Attorney General or the prosecuting attorney for each county, or a subordinate designated to act in either absence or incapacity, may apply in writing under oath or equivalent affirmation to a circuit court judge designated by the chief of justice of the Hawaii supreme court or any other circuit court judge or district court judge, if a circuit court judge has not been so designated or is otherwise unavailable, for an order or extension of an order to authorize the installation and use of a pen register or a trap and trace device. The application shall include: (a) the identity of the official making the application and the law enforcement agency conducting the

April 2003]

STATE WIRETAP LAWS

1025

investigation; and (b) the facts and circumstances relied upon the applicant to conclude that there is probable cause to believe that information will be obtained through the installation and use of a pen register or trap and trace device which will constitute the fruits, instrumentalities, or evidence of a crime covered under this part. (803-44.5).

Order:

An order authorizing installation and use of pen register or a trap and trace device shall not be for a period exceeding sixty days. Extension of such an order may be granted, but only upon a reapplication for an order and a finding of probable cause to justify continuing use of a pen register or trap and trace device. The period of the extension shall not exceed sixty days. (803-44.6(c)).

An order authorizing the installation and use of a pen register or a trap and trace device shall direct that: (1) the order be sealed until otherwise ordered by the court; and (2) the person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless otherwise ordered by the court. (803-44.6(d)).

STORED ELECTRONIC COMMUNICATIONS:

A governmental entity may require disclosure of the contents of an electronic communication that has been in electronic storage for 180 days, or less, from the provider of the electronic communication service where storage has taken place, only by means of a search warrant. A governmental entity may require disclosure of the contents of an electronic communication which has been in electronic storage for more than 180 days by requiring provider of remote computing services to disclose the contents of certain electronic communications without notice to the subscriber or customer, if a search warrant has been obtained; or with prior notice to the subscriber or customer, if a court order for disclosure has been obtained, except that delayed notice maybe authorized by the order. Such electronic communication subject to disclosure includes communications held or maintained on a remote computing service: (1) on behalf of, and received by electronic transmission from (or created by computer processing of communications received by electronic transmission from) a subscriber or customer of such remote computing service, and (2) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such

April 2003]

STATE WIRETAP LAWS

1027

intercepted; a particular description of the type of communications sought to be intercepted; the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (e) a full and complete statement of the facts concerning all previous applications known to the individual making the applications, made to any judge for authorization to intercept wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. (18-6708(1)).

Order:

The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. Upon such application, the judge may enter an *ex parte* order, as requested or as modified, authorizing interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting if the judge determines on the basis of the facts submitted by the applicant that: (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular enumerated offense; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. (18-6708(2)–(3)).

Each order authorizing the interception of any wire or oral communication must specify: the identity of the person, if known, whose communications are to be intercepted; the nature and location of the communications facilities as to which, or the place where,

authority to intercept is granted; a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; the identity of the agency authorized to intercept the communications, and of the person making the application; and the period of time during which such interception is authorized, including a statement as to whether or not the interception must automatically terminate when the described communication has been first obtained. (18-6708(4)).

An order authorizing the interception of a wire or oral communication must, upon request of the applicant, direct that a communications common carrier, landlord, custodian, or other person must furnish the applicant with all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such communications common carrier, landlord, custodian or person is providing the person whose communications are to be intercepted. Any communications common carrier, landlord, custodian or other person furnishing such facilities or technical assistance must be compensated therefor by the applicant at the prevailing rates. (18-6708(5)).

No order entered may authorize the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with the procedures stated above and the court making the findings required above. The periods of extension must be no longer than the authorizing court deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days for each extension. Every order and extension must contain a provision that the authorization to intercept be executed as soon as practicable, be conducted in such a way as to minimize the interception of communications not otherwise subject to interception, and terminate upon attainment of the authorized objective, or in any event in thirty days. (18-6708(6)).

Reports:

Whenever an order authorizing interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports must be made at such intervals as the judge who may require. (18-6708(7)).

April 2003]

STATE WIRETAP LAWS

1029

PEN REGISTER/TRAP & TRACE DEVICE:*Application:*

An application for an order or an extension of an order authorizing or approving the installation of a pen register or trap and trace device may be made by a prosecuting attorney or Attorney General, and the application should provide the names of the prosecuting attorney or Attorney General making the application, the identity of the law-enforcement agency conducting the investigation and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation conducted by that agency. The statute exempts electronic or wire communication service providers who install such devices in the regular course of their business or who are cooperating with law enforcement officers pursuant to an *ex parte* order. (18-6721, 18-6723).

Order:

An order shall: specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; specify the identify, if known, of the person who is the subject of the criminal investigation; specify the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of the trap and trace device, the geographic limits of the trap and trace order; contain a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and direct, upon the request of the application, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. (18-6722(2)).

An order issued to install a pen register or trap and trace device is valid only for a period of sixty days. An order may be extended with an application containing all information required in original application and upon same judicial findings and may not exceed sixty days. (18-6722(3)).

An order authorizing the installation and use of a pen register or a trap and trace device shall direct that: (A) the order be sealed until otherwise ordered by the court; and (B) the person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed

attempting to commit a controlled substance offense) has been, is being, or may be committed. The affidavit must describe the nature of the location of the facility or place from which the communication is to be intercepted. It must also identify, if known, the person allegedly committing the offense whose communication is to be intercepted and the type of communication to be intercepted. The application must include a statement specifying that other investigative procedures have been tried and failed or may not succeed or are too dangerous to attempt and a statement of duration necessary for the interception. It must also describe any previous applications for a warrant and the court's action on any such application. The application need not specify that the interception is likely to yield communications related to the crime. (35-33.5-2-2).

A court in the county where the prosecuting attorney is located or where the communication is subject to the warrant is anticipated to be received or sent may grant an order authorizing a warrant under exigent circumstances that require "the preservation of secrecy" or if probable cause exists to believe the person whose communications are to be intercepted is committing, has committed or may commit a designated offense (described above). A court also may enter an order authorizing a warrant if communications concerning the designated offense identified in the warrant application are likely to be obtained through an interception. The court must also find that the place or facility from which the communications are to be intercepted is being used by, listed in the name of, leased to, or commonly used by a person who is committing, has committed or may commit a designated offense. The court must also find that investigative procedures have been tried and failed or are unlikely to succeed or are too dangerous to attempt. (35-33.5-3-1).

Order:

A warrant or extension may authorize interception for no more than fourteen days. The warrant must identify the law enforcement agency that the warrant directs to make the interception, the identity of the person, if known, whose communication is to be intercepted, the nature and location of the facility or place from which the communication is to be intercepted, the type of communication to be intercepted and a statement of the designated offense to which the communication relates. (35-33.5-3-2).

(There are no provisions for obtaining a warrant in emergency circumstances.)

A warrant may be extended three times for periods of not more than fourteen days. To obtain an extension, a new application must be filed with the court. The rules do not specify whether the warrant can be extended to include crimes not listed in the original order,

however, an extension may only be given with respect to designated offenses. (35-33.5-4-1).

Law enforcement officer may disclose the contents of an interception to another law enforcement officer only to the extent that disclosure is appropriate to the proper performance of the law enforcement officer's official duties. (35-33.5-5-3).

Reports:

The court shall order that reports be submitted to the court indicating the progress that has been made toward the authorized objective and whether continued interception is necessary. The court may establish the times when a report is required. (35-33.5-4-2).

A prosecuting attorney, no later than December 31 of each year, must report to the legislative council the fact that a warrant or extension was applied for, the type of warrant, whether the warrant was granted, modified or denied, the duration authorized for interception, the designated offense for which the warrant was issued, the persons who applied for the warrant and the nature of the place from which communications were to be intercepted, the arrests resulting from interception, among other things. (35-33.5-2-4).

Within twenty-eight days after the termination of a warrant or extension, or the denial of an application for a warrant or extension, the court shall submit to the executive director of the division of the state court administration containing: the fact that the warrant or extension was applied for, the type of warrant or extension applied for, the fact that the application for a warrant or extension was granted, the duration authorized for interception and the number of extensions, the designated offense, the identity of the persons who applied, the nature and location of the place or facility from which the communications were intercepted, and the reasons for withholding notice from the person whose call was intercepted, if notice was withheld. (35-33.5-2-5).

STATE: IOWA
IOWA CODE §§ 727.8, 808B.3-
B.14 (1994)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The application shall be in writing upon oath or affirmation to a court. It shall include the identity of the special state agent

April 2003]

STATE WIRETAP LAWS

1033

requesting the application, the supervisory officer reviewing and approving the request, and the approval of the administrator of the department of public safety under whose command the special state agent is acting; a full and complete statement of the facts and circumstances relied upon by the applicant to justify the belief that an order should be issued, including details of the particular offense, a description of the nature and location of the facilities from which or the place where the communication is to be intercepted, a particular description of the type of communication to be intercepted, and the identity of the person, if known, committing the offense whose communications are to be intercepted; a statement as to whether other investigative procedures have been tried and failed or why they reasonably appear unlikely to succeed if tried or to be too dangerous; a statement of the period of time for which interception is required to be maintained; a statement of the facts concerning previous applications and the action taken on those applications; if the application is for an extension of an order, a statement setting forth the results thus far obtained or a reason for failure to obtain results. (808B.5(1)).

Order:

Upon application, the court may enter an *ex parte* order authorizing the interception of wire, oral, or electronic communications within the territorial jurisdiction of the court if it finds: probable cause for the belief that an individual is committing, has committed, or is about to commit a felony offense involving dealing in controlled substances; normal investigative procedures have failed or reasonably appear unlikely to succeed if tried or be too dangerous; there is probably cause for belief that the facilities from which, or the place where the wire, oral, or electronic communications are to be intercepted are being used, are about to be used, in connection with the commission of the offense or are leased to, listed in the name of, or commonly used by the person whose communications are to be intercepted. (808B.5(3)).

Any such order shall not authorize interception for a longer period than is necessary or in any event longer than thirty days. (808B.5(6)).

An extension of an order may be granted but only upon application for an extension setting forth the information described above. The period for the extension shall be no longer than the authorizing court deems necessary, but in no event longer than thirty days. There is no provision regarding whether an order can be extended to cover crimes not listed in the order. An extension will only be granted for the enumerated felonies set forth above. (808B.5(6)).

PEN REGISTER/TRAP & TRACE DEVICE:*Application:*

A person shall not install or use a pen register or a trap and trace device without first obtaining a court order. However, a pen register or a trap and trace device may be used or installed without court order if any of the following apply: (a) it relates to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of the provider of the service, or to the protection of users of the service from abuse of the service or unlawful use of the service; (b) if a wire or electronic communication was initiated or completed in order to protect the provider of the wire or electronic communication service, another provider furnishing service toward the completion of the wire or electronic communication, or a user of the service, from fraudulent, unlawful, or abusive use of the service; (c) if consent was obtained from the user of the electronic or wire communication service. (808B.10).

An application for an order or extension of an order authorizing or approving the installation or use of a device shall be made in writing by a prosecuting attorney upon oath or affirmation to a district court. Only a special agent may conduct an investigation using such a device. The application shall include information regarding: the identity of the person who owns or leases the line where the device will be attached; the identity of the person subject to a criminal investigation; the telephone number and physical location of the telephone line; the period of time for which authorization is sought shall not exceed sixty days. (808B.11).

Emergency:

In an emergency, the issuance of a pen register or trap and trace order may be based upon sworn oral testimony communicated by the director of criminal investigation, the director of narcotics enforcement, a special state agent authorized by the prosecuting attorney, or the prosecuting attorney, via the telephone, if the judge who is asked to issue the order is satisfied that the circumstances make it reasonable to dispense with a written affidavit. A pen register or trap and trace device may only be installed and used if both of the following occur: (a) the court reasonably determines that an emergency situation exists that involves an immediate danger of death of or serious injury to any person; (b) a written order approving the installation or use of a pen register or trap and trace device is obtained within forty-eight hours of the issuance of an order. In the absence of an authorizing order, an emergency order shall

April 2003]

STATE WIRETAP LAWS

1035

immediately terminate upon the earlier of obtainment of information sought, denial of the application, or the lapse of forty-eight hours after the authorization of the installation of the pen register or trap and trace device. (808B.12).

An order may be extended for up to sixty days upon application. (808B.11).

Reports:

The order authorizing interception may require that reports be made to the court which issued the order showing what progress has been made toward achievement of the authorized objectives. (808B.5(7)).

In January of each year, the Attorney General and the county attorneys shall report to the state court administrator the number of pen register orders for trap and trace devices applied for and obtained by their offices during the preceding calendar year. (808B.14).

Within thirty days after the denial of an application or after the expiration of an order granting an application, or after an extension of an order, the court shall report specified details to the state court administrator. (808B.6(1)).

In January of each year, the Attorney General and the county attorneys shall report to the state court administrator and to the Administrative Offices of the United States district courts enumerated details about interception requests and orders granted and arrests made as a result of such orders. (808B.6(2)).

STATE: KANSAS

PARTY CONSENT: One

KAN. STAT. ANN. §§ 17-1908, 21-

LEGISLATION: Yes

4001, 22-2514-2516 (2001)

CURRENT LAW

WIRETAP:

Application:

The application must be made in writing, upon oath or affirmation, to a judge of competent jurisdiction, and must state the applicant's authority to make the application. It must also include the identity of the prosecuting attorney, and the officer requesting that the application be made; a full statement of the facts and circumstances including (a) details about offense; (b) a description of the facilities; (c) a description of the type of communication to be intercepted; (d) the identity of the person committing the offense. It

must also include a statement as to whether other investigative procedures have been tried and failed or appear reasonably unlikely to succeed if tried or be too dangerous; a statement of the period of time for which authorization is sought; a statement of the facts concerning all previous applications and the action taken on each; and where the application is for an extension, a statement setting forth the results thus far or a reasonable explanation of the failure to obtain results. (22-2516(1)).

The judge may require additional testimony or documentary evidence. The judge may issue an *ex parte* order if he or she determines that there is probably cause to believe a person is committing, has committed or will commit one of the enumerated offenses; particular communications concerning the offense will be obtained through such interception; normal investigative procedures have been tried and failed or appear reasonably unlikely to succeed if tried or be too dangerous; and that the facilities from which the communications are to be intercepted are being used or are about to be used in connection with the commission of such offense or are leased to or commonly used by such person. (22-2516(21)).

Order:

The order shall specify the identity of the person whose communications are to be intercepted, nature and location of facilities; identity of agency authorized to intercept; period of time for which interception is authorized and a statement as to whether the interception shall automatically terminate once the communication has been obtained; direct landlord, public utility or other to assist. (22-2516(4)).

No order shall authorize interception for a period exceeding thirty days. (22-2516(5)).

Orders may be extended based on a new application containing the information set forth above, and may be extended for no longer than thirty days. (22-2515(b)).

Any investigative or law enforcement officer who, by any means authorized by state or federal law, has obtained knowledge of the contents of any wire, oral or electronic communication, or evidence derived therefrom, may disclose contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. (22-2515(b)).

Any investigative or law enforcement officer who has obtained knowledge of the contents of any communication, or evidence derived therefrom, may use such contents to the extent such use is appropriate to the proper performance of such officer's official duties. (22-2515(c)).

April 2003]

STATE WIRETAP LAWS

1037

When an investigative or law enforcement officer, while engaged in intercepting wire, oral or electronic communications, intercepts communications relating to offenses other than those specified in the order authorizing the interception of the wire, oral or electronic communication, the contents and evidence derived therefrom may be disclosed or used. Such contents and evidence derived may be used when authorized by a judge of competent jurisdiction, where such judge finds on subsequent application, made as soon as practicable, that the contents were intercepted in accordance with the act's provisions. (22-2515(f)).

Reports:

The issuing judge may require reports to be made showing what progress has been made toward the objective. (22-2516(6)).

Within thirty days after the expiration of an order or any extension thereof, the judge issuing such order shall report to the Administrative Office of the U.S. courts information as is required to be filed by 18 U.S.C. § 2519. A duplicate copy of such report shall be filed with the judicial administrator of the courts of this state. (22-2519(1)).

In January of each year, the Attorney General and each district attorney and county attorney shall report to the Administrative Office of the United States courts such information as required by 18 U.S.C. § 2519. A duplicate copy of such report shall be filed with the judicial administrator of the courts of this state. (22-2519(2)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

An attorney for the government or an investigative or law enforcement officer may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device to a court of competent jurisdiction. Such application shall be in writing and shall be under oath or equivalent affirmation. An application shall include: (a) the identity of the attorney for the government or the investigative or law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and (b) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. (22-2526).

April 2003]

STATE WIRETAP LAWS

1039

STATE: LOUISIANA **PARTY CONSENT:** All
LA. REV. STAT. ANN. §§ 14:322, **LEGISLATION:** Yes
15:1304–1316 (West 1992)

CURRENT LAW**WIRETAP:***Application:*

The Attorney General, with the approval of the district attorney in whose district the interception of wire or oral communications takes place, and the district attorney, with the approval of the Attorney General, may authorize an application to a judge in whose district the interception of wire or oral communications shall take place, and such judge may grant an order authorizing or approving the interception of wire or oral communications by an investigative or law enforcement officer having responsibility for the investigation of the offense for which the application is made, when such interception may provide or has provided evidence of: any violation of the Uniform Controlled Dangerous Substances Act by producing, manufacturing, distributing, or dispensing a controlled dangerous substance; or possessing with intent to produce, manufacture, distribute, or dispense a controlled dangerous substance; or creating, distributing, or possessing a counterfeit controlled dangerous substance; or conspiring to commit any of the above enumerated offenses. Interception orders may be granted when they provide evidence of the commission, attempted commission, or conspiracy to commit a crime involving any of the following offenses: first or second degree murder; aggravated kidnapping; aggravated arson; manufacture and possession of delayed action incendiary device or manufacture and possession of a bomb; armed robbery; jury tampering; solicitation for murder; arson with intent to defraud; extortion; felony violations of the Uniform Controlled Dangerous Substances Act; intimidating, impeding, injuring witnesses or injuring officers; any felony offense where the offense was or is to be committed against a law enforcement officer as a result of his official capacity or actions; money laundering; transactions involving proceeds from drug offenses. (15:1308).

Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge in whose district such interception of wire or oral communication shall take place and shall state the applicant's authority to make such application. Each application shall

include the following information: (a) the identity of the investigative or law enforcement officer making the application and the person authorizing the application; (b) a full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued, including: (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, and (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous, or that such circumstances exist that without immediate action a human life may be endangered; (d) a statement of the period of time for which the interception is required to be maintained, which shall not exceed thirty days, (e) when the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results; (f) a full and complete statement of the facts concerning previous applications for the past five years, known to the individuals authorizing and making the application, made to any judge for authorization to intercept, or for approval of interception of, wire or oral communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application. If statements of an identified or unidentified informant are relied upon in the application as a basis for establishing that there are reasonable grounds to believe that an offense has been, is being, or is about to be committed, the application shall set forth the factual basis for the affiant's belief that the informant is credible and that the information has been obtained in a reliable manner. The informant shall be presented to the judge and be sworn to afford the judge opportunity to inquire if the statements made in the application are true. The application shall so state that the informant was presented to the judge and sworn for such purpose. This provision shall not affect the privileged character of the identity of an informant. Nothing herein shall be construed to require the identification of a confidential informant. (15:1310(A)-(B)).

Order:

Upon such application, the judge may enter an *ex parte* order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the

district in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that: (1) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated; (2) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (3) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense or are leased to, listed in the name of, or commonly used by such person; (4) there is reason to believe that investigative procedures have been tried and failed or they reasonably appear to be unlikely to succeed if tried or to be dangerous, or that such circumstances exist that without immediate action a human life may be endangered; (5) the interception of wire or oral communications, as planned, is not reasonably expected to intercept privileged communications.

Each order authorizing or approving the interception of any wire or oral communication shall specify: (1) the identity of the person, if known, whose communications are to be intercepted; (2) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (3) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates; (4) the identity of the agency authorized to intercept the communications, the person applying for the application, and the person authorizing the application; (5) the period of time during which such interception is authorized. (15:1310(c)-(d)).

No order may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the investigation, and in no event longer than thirty days. (15:1310(E)).

Extensions of an order may be granted, but only upon application for an extension upon an application containing the information described above and the court's making the findings described above. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty successive days or until the described type of communication has been obtained. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception, and must terminate upon completion of the investigation or expiration of the order. (15:1310(E)).

Reports:

Whenever an order authorizing the interceptions is entered, the order shall require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require. (15:1310(F)).

Within twenty days after the expiration of an order, an extension, or the denial of an order approving an interception, the issuing or denying judge shall report to the judicial administrator of the supreme court certain details about the type of order and its contents, including the offense specified in the order or application, or extension of an order and the nature of the facilities from which or the place where communications were to be intercepted. (15:1311(A)).

In January of each year, the district attorneys shall report to the Attorney General and in March of each year the Attorney General shall report to the judicial administrator of the supreme court information about interceptions including a general description of the interceptions made and the nature and frequency of incriminating communications intercepted. (15:1311(B)).

Each April, the judicial administrator of the supreme court report to the legislature concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and the number of orders and extensions granted or denied during the preceding calendar year. The report shall include a summary and analysis of the data filed with the judicial administrator. (15:1311(C)).

The head of each law enforcement agency that possesses or makes applications for installation and use of a pen register or trap and trace devices must ensure that a designated officer transmits no later than March first of each calendar year to the deputy secretary of public safety services of the Department of Public Safety and Corrections, a sworn affidavit stating that all installations and uses of the pen register or trap and trace devices have been in accordance with the statute and that no pen register or trap and trace device in the custody of that agency has been the subject of an unauthorized or illegal installation or use. (15:1315(E)(4)).

PEN REGISTER/TRAP & TRACE DEVICE:*Application:*

An investigative or law enforcement officer may apply for an order or an extension of an order to a court of competent jurisdiction

April 2003]

STATE WIRETAP LAWS

1043

authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of this state. For these purposes, "investigative or law enforcement officer" means: (1) any state police officer; (2) any full-time city police officer of a state municipality; (3) any sheriff or a deputy sheriff of a state parish, which has been designated by the sheriff of that parish as responsible for preparation of applications for installation and use of pen register or trap and trace devices. The application must include the identity of the investigative or law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation. A certification by the applicant attesting that the information sought is relevant to an ongoing felony criminal investigation being conducted by that agency, and includes in that certification a recital of facts or information constituting the reasonable suspicion upon which the application is based. And a certification by the appropriate agency head that he has reviewed the application and approves the use of the pen register or trap and trace device for that investigation. (15:1314).

Order:

The court may enter an *ex parte* order authorizing installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the investigative or law enforcement officer has certified to the court that the information likely to be obtained is relevant to an ongoing felony criminal investigation, and that the certification includes "reasonable suspicion." (15:1315(A)).

An order shall specify: (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (b) the identity, if known, of the person who is the subject of the criminal investigation; (c) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of trap and trace, the geographic limits of the trap and trace order; (d) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates. An order shall direct, upon request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. (15:1315(B)).

An order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed ten days. (15:1315(C)(1)).

Extensions of such an order may be granted, but only upon an application for an order described above and upon the judicial findings set forth above. The period of extension shall be for a period not to exceed ten days. (15:1315(C)(2)).

STATE: MAINE
ME. REV. STAT. ANN. tit. 15,
§§ 709–713 (2003)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

Maine lacks a comprehensive statutory system regarding the interception of wire, oral or electronic communications.

STATE: MARYLAND
MD. CODE ANN., CTS. & JUD.
PROC. §§ 10-401 to 10-4B-05
(2002)

PARTY CONSENT: All
LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Application:

The Attorney General, state prosecutor, or any state's attorney may apply to a judge of competent jurisdiction for wiretap order when the interception may provide evidence of the commission of certain enumerated offenses (e.g., murder, kidnapping, rape, child abuse, gambling, robbery, fraudulent insurance acts, etc.). The order applies only within the territorial jurisdiction of the authorizing court. However, if the interception relates to a mobile phone or pager, the order can cover transmissions within the entire state, but the application must allege the offense being investigated happened in the court's territory. (10-406(a)).

Application for a wiretap order must be made in writing upon oath or affirmation to a circuit court judge and shall state the applicant's authority to make the application. Each application must contain: (a) the identity of the officer, (b) a full and complete statement of the facts/circumstances, (c) a full and complete statement as to whether other investigative procedures have been tried and failed and why, (d) the period of time the wiretap is needed, (e) a full and complete statement of the facts concerning all previous applications involving the same persons, facilities, places and the action taken by the judge in those cases, (f) if an extension an explanation as to the failure to obtain results, and (g) any additional

April 2003]

STATE WIRETAP LAWS

1045

information required by the judge. Issuance of the order requires probable cause of a crime and the particular location is the correct place for the wiretap that the interception will produce particular communications, normal investigative procedures have been tried and failed or reasonably appear to likely be unsuccessful or too dangerous. Wiretap must stop upon intercepting the authorized objective, but no longer than thirty days. Additional thirty-day extensions may be granted. (10-408).

Order:

Upon the application, the judge may enter an *ex parte* order, as requested or as modified, authorizing interception of wire, oral, or electronic communications within the territorial jurisdiction permitted under the statute, if the judge determines on the basis of the facts submitted by the applicant that: (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through the interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and (d) there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by this person. An *ex parte* order may authorize the interception of wire, oral, or electronic communications only within the territorial jurisdiction of the court in which the application was filed. If an application for an *ex parte* order is made by the Attorney General, the State Prosecutor, or a State's Attorney, an order may authorize the interception of communications received or sent by a mobile telephone or a paging device anywhere within the State so as to permit the interception of the communications regardless of whether the mobile telephone or paging device is physically located within the jurisdiction of the court in which the application was filed at the time of the interception. The application must allege that the offense being investigated may transpire in the jurisdiction of the court in which the application is filed. (10-408(c)).

Each order authorizing the interception of any wire, oral, or electronic communication shall specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) a particular description of the type of communication sought to be intercepted, and a statement

of the particular offense to which it relates; (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and (e) the period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (10-408(d)).

An order entered may not authorize the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. The thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. (10-408(e)).

Extensions of an order may be granted, but only upon application for an extension containing the information set forth above and the court making the findings described above. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. (10-408(e)).

Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this subtitle, and must terminate upon attainment of the authorized objective, or in any event in thirty days. (10-408(e)).

Reports:

Progress reports regarding the interception must be submitted to the authorizing judge (intervals of which are set by judge). (10-408(f)).

Judges must submit report within thirty days of expiration or denial of an order to the Administrative Office of the courts. Attorney General, state prosecutors, and state's attorneys must submit annual reports to the Administrative Office of the courts. Based upon this information, the Administrative Office of the courts will prepare and submit a report to the state General Assembly. (10-409).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

An investigative or law enforcement officer may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace

April 2003]

STATE WIRETAP LAWS

1047

device, in writing, under oath or equivalent affirmation, to a court of competent jurisdiction of Maryland. An application shall include: (a) the identity of the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (b) a statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. (10-4B-03).

Order:

Upon an application, the court shall enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation. An order shall: (1) specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (2) specify the identity, if known, of the person who is the subject of the criminal investigation; (3) specify the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; (4) contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and (5) direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. An order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. (10-4B-04).

Extensions of an order issued under this section may be granted upon a new application for an order and upon the judicial finding described above of this section. An extension may not exceed sixty days. (10-4B-04).

An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that: (1) the order be sealed until further order of the court; and (2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

STORED ELECTRONIC COMMUNICATIONS:

A person may not obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in an electronic communications system by: (1) intentionally accessing without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeding an authorization to access a facility through which an electronic communication service is provided. A person who violates these provisions is subject to the following penalties: (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, (i) for a first offense, a fine of not more than \$250,000 or imprisonment for not more than 1 year, or both; and (ii) for a second or subsequent offense, a fine of not more than \$250,000 or imprisonment for not more than two years, or both; or (2) in any other case, a fine of not more than \$5,000 or imprisonment for not more than 6 months, or both. (10-4A-02(a)-(b)).

A person or entity providing an electronic communication service to the public may not knowingly divulge to any other person or entity the contents of a communication while the communication is in electronic storage by that service. Except as otherwise provided, a person or entity providing remote computing service to the public may not knowingly divulge to any other person or entity the contents of any communication which is carried or maintained on that service: (i) on behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service; and (ii) solely for the purpose of providing storage or computer processing services to a subscriber or customer, if the provider is not authorized to access the contents of any communications for purposes of providing any services other than storage or computer processing. A person or entity may divulge the contents of a communication: (a) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient; (b) if authorized under the provisions of this subtitle; (c) with the lawful consent of the originator or an addressee or intended recipient of the communication, or the subscriber in the case of remote computing service; (d) to a person employed or authorized or whose facilities are used to forward the communication to its destination; (e) if necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (f) to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime. (10-4A-03).

April 2003]

STATE WIRETAP LAWS

1049

An investigative or law enforcement officer may require a provider of electronic communication service to disclose the contents of an electronic communication that is in electronic storage in an electronic communications system for 180 days or less, only in accordance with a search warrant issued by a court of competent jurisdiction. An investigative or law enforcement officer may require a provider of electronic communications services to disclose the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days. (10-4A-04).

STATE: MASSACHUSETTS **PARTY CONSENT:** All
MASS. ANN. LAWS ch. 272, § 99– **LEGISLATION:** Yes
99A (Law. Co-op. 2000)

CURRENT LAW**WIRETAP:***Application:*

The Attorney General, any assistant Attorney General designated by the Attorney General, any district Attorney General, or any assistant district Attorney General designated by the district attorney, may apply for a warrant to initiate interception. The application must be in writing and sworn by the applicant. An application for an interception warrant may be issued only upon (a) a sworn application; (b) probable cause that a designated offense has been, is being, or is about to be committed and that the intercepted information will aid in apprehending the defendant; and (c) a showing that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried. The application must also include:

- A statement of facts establishing probable cause that a designated offense has been, is being, or is about to be committed.
- A statement of facts establishing probable cause that interception provide evidence or aid in apprehending a person who has committed, is committing or about to commit a designated offense.
- The place and premises where the oral or wire communications will occur.
- A description of the nature of the oral or wire communications to be obtained.

- A statement that the communications is not privileged and are material to the investigation or prosecution.
- A statement concerning the time period (if known) of the warrant and a statement showing probable cause that the described communications will continue and that the order should not terminate when the communications is first obtained.
- A statement whether secret entry on a private place is necessary.
- Disclosure of previous applications or warrants.
- A statement showing good cause to postpone service. (99(F)(2)).

The application must designate an offense and relate to the following enumerated offenses: arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming, intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subordination of perjury, any violation of interception laws, being an accessory to any of the foregoing offenses, and conspiracy or attempt or solicitation to commit any of the foregoing offenses. (99(B)).

The applicant, or any law enforcement officer designated by the applicant, may execute the warrant order. Investigative or law enforcement officer means any “any officer of the U.S., a state or political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses.”

Order:

A judge of competent jurisdiction of the county where interception is to occur, the county where the office of the applicant is located, or, if there is not judge of competent jurisdiction, to the judge of competent jurisdiction sitting in Suffolk county is authorized to issue a warrant order. (99(G)).

- The warrant must contain:
- The name of the issuing judge.
- The issued, effect, and termination date.
- A description of the person and place, premises, or telephone line to be intercepted.
- A description of the nature of the oral or wire communications to be obtained through interception and including a statement to the offenses that they relate.
- An express authorization (if applicable) to allow a secret entry into private premises to install an intercepting device.

- A statement providing for service of the warrant on the person to be intercepted. (99(I)).

The warrant is good for anywhere in the state and maybe executed only pursuant to its terms (e.g., hours, time period). A warrant is effective for thirty days or when the targeted communication is intercepted (unless the warrant states otherwise). However, a warrant to permit oral or wire interception cannot exceed fifteen days. The date of installation of a physical device starts the thirty-day clock. (99(I)).

The statute does not provide for interception in emergency cases. However, an application must be renewed before the warrant's original expiration date and only for an additional fifteen-day period (renewal is not for another thirty-day period). The renewal application must incorporate the initial warrant order and application and set forth the progress to date on the initially authorized interception. In addition, the applicant must present grounds for extending the warrant order. (99(J)).

Reports:

Within seven days after the warrant's expiration/termination, a report must be filed with the issuing judge that provides:

Nature and location of the communications facilities and premise/places where interceptions were made; the periods of time during which such interceptions were made; the names of the parties to the communications intercepted; the original recording of the oral or wire communications intercepted; and an attested statement of each person who heard the intercepted communications that was not recorded pursuant to the warrant. (99(M)).

On the second Friday of each January, the Attorney General and each district Attorney General is required to submit a report to the court providing: the number of applications made; the name of the applicant; the number of warrants issued; the effective period of the warrants; the number and designation of the offenses provided in the application; the number of renewals; the number of interceptions made; the number of indictments obtained; and the number of criminal convictions.

A copy of the Attorney General's report must be kept and made available to the public. The statute makes no reference to reports to the federal government. (99(R)).

April 2003]

STATE WIRETAP LAWS

1053

intercepting communication; any other limitations; statement that using or divulging intercepted communications is unlawful and punishable; and statement that warrant should be executed as soon as possible (the thirty-day period begins on day of commencing interception or ten days after the order is received by law enforcement or agency). The warrant may also indicate if assistance of landlord, custodian, or other person is required to undertake interception. (626A.06(4)).

The interception is good for the territorial jurisdiction of the court, valid when the described communication is obtained, or valid up to thirty days, with additional thirty-day extensions. An extension application requires information required for an initial application, and a judge of competent jurisdiction must make a finding that there is probable cause to issue a warrant order. In addition, the extension application must contain a statement of the progress of interception activities. (626A.06(4)).

Emergency:

Emergency interceptions that involve immediate danger to death or serious physical injury may commence when oral approval given by a judge of competent jurisdiction; a written application must be submitted within thirty-six hours after commencing interception. (626A.065).

Reports:

An issuing judge may require periodic reports to assess progress in intercepting communications under the warrant order. (626A.06(8)).

The judge shall submit within thirty days after the termination of the order (or denial of the application) various information regarding the application/interception to the state court administrator. Information must include: kind of order or extension applied for; whether application was granted as applied for, modified, or denied; the time period for interceptions or use of a pen register and trap and trace device; offenses specified in the order; identity of the law enforcement officer or investigative agency; and nature of the facilities from where communications is to be intercepted. (626A.17(1)).

The county attorney shall submit a report by January 15 to the state court administrator information that includes the following: with respect to each order issued the information listed above that is required by the issuing judge; general description of interceptions made under each order/extension, including: nature/frequency of incriminating communications; nature/frequency of other intercepted communications; number of persons whose communications were

intercepted; nature, amount and cost of manpower and other resources used in interception. the number of arrests, trials, motions to suppress, and convictions resulting from interception. (626A.17(2)).

The state court administrator shall bi-annually submit to the state legislature a report regarding the application for and use of interceptions during the previous two years. Report must be made available to the public at the legislative reference library and the state's court administrator's office. (626A.17(3)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

Use of pen register, trap and trace, or mobile tracking device requires court order. The application for a pen register, trap and trace or mobile tracking is generally less burdensome than that for wiretap. An application requires the identity of the law enforcement officer and the identity of the law enforcement agency conducting the investigation and a statement of facts and circumstances relied upon in justifying the application. Order is good for the jurisdiction of the court (or, in the case of a mobile tracking device, good outside of the jurisdiction of the court as long as the device is installed in the jurisdiction). An order must include: identity (if known) of the person to whom is leased or in whose name is listed the telephone line; number and physical location of the telephone line if pen register or trap and trace device or objects to be attached in the case of mobile tracking device, and geographic limits of the trap and trace order; a statement of the offense; identity of the law enforcement officer responsible for installation; time period of the order; and statement whether landlord or other persons must assist in installation. (626A.36).

Order good for sixty days and extensions made before warrant expiration that includes the six items list above. (626A.37(3)).

STORED ELECTRONIC COMMUNICATIONS:

A governmental entity must first obtain a warrant to obtain the contents of information stored in an electronic communication service for 180 days or less. The following procedure applies if the content of information has been stored for 180 days or more (or it involves a remote computing service): warrant—if a governmental entity obtains a warrant, no notice is required to the subscriber/customer; or administrative subpoena or court order—if a governmental entity obtains an administrative subpoena or court order, notice is required to the subscriber/customer. (626A.28(1)-(2)).

days); statement whether covert entry is necessary to install intercepting device; and statement of other applications previously made involving the same person, facility, or places specified in the application. (41-29-505, 41-29-513).

Upon receipt of the above information from the director of the Bureau, the prosecutor is authorized to submit an application to a judge of competent jurisdiction. The application must be in writing, under oath, and contain the above listed information. (41-29-515(4)).

Applicants may extend initial interception order for another thirty-day period. Extension application must show to date the results from the initial interception order or a reasonable explanation on the failure to obtain results.

Order:

The order for interception must specify: identity of the person (if known) whose communications are to be intercepted; nature and location of the communication facilities; description of the type of communication to be intercepted and a statement of the particular offense to which it relates; statement setting forth the identity of the prosecutor and a statement that the director has authorized the prosecutor to make an application; time period of the interception order (no longer than thirty days) and a statement whether or not interception will terminate when the described communication is first obtained; and statement whether covert entry is necessary. (41-29-515(2)).

Reports:

A judge may require a periodic report by the applicant to monitor the progress of interception activity. (41-29-515(8)).

Reports required by judge and prosecuting attorney to Administrative Office of the U.S. Courts pursuant to federal law. In addition, judges and prosecutors are required to send copies of the reports to the director of the Bureau. On or before January 5, the director of the Bureau is required to submit a report to the Mississippi Administrative Office of Courts that has the following: report of judges and prosecuting attorneys forwarded to the director; the number of Bureau personnel authorized to possess, install, or operate electronic, mechanical, or other devices; the number of Bureau and other law enforcement personnel who participated or engaged in the seizure of intercepts; the total cost to the Bureau of all activities and procedures relating to the seizure of intercepts during the preceding year, including costs of equipment, manpower, and expenses incurred as compensation for use of facilities or technical assistance provided by the Bureau. (41-29-527(3)).

o be too dangerous; time period (no longer than thirty days) and a statement why interception should not end when the targeted communication is intercepted; statement of previous applications involving the same persons, facilities, or places specified in the application; and statement that adequate resources are available to conduct interception. (542.408(1)).

Order:

An *ex parte* order issued by the judge (only for the territorial jurisdiction of the court) must contain: identity of the person and employment (if known); nature and location of the communications facilities; identity of the agency authorized to intercept communications; and time period (no longer than thirty days) and whether interception ceases when described communication is first obtained. (542.408(5)).

Applicants may apply for an extension request and must provide information on results of interception activities. (542.408(5)).

Reports:

The judge issuing the interception order may request periodic progress reports of the interception. (542.408(6)).

Issuing judges must submit report within thirty days of expiration or denial of an order to the state courts administrator. The report must contain: kind of order/extension applied for; whether order was granted, modified, or denied; offense specified in the order/application; identity of the investigative officer and person making the application; nature of the facilities. (542.416(1)).

By January of each year, the principal prosecuting attorney must report: all the information listed above; description of interceptions, (which must include the nature and frequency of incriminating statements; nature and frequency of other communications; number of persons intercepted; nature and cost of manpower used; number of arrests, trials, motions to suppress, convictions resulting from interceptions; and general assessment of importance of interceptions). (542.416(2)).

In April of each year, the state courts administrator is required to submit a report to the Missouri general assembly of the number of applications for orders approving wire interceptions and number of extensions granted or denied. In addition, state courts administrator must provide in summary analysis form all of the information required to be submitted by the issuing court and prosecuting attorney (listed above). (542.416(3)).

(if known) committing the offense and whose communications is to be intercepted; statement whether other investigative procedures have been tried and failed or why they reasonably appear unlikely to succeed if tried or to be too dangerous; time period and statement whether interception automatically terminates when objective is met; and statement concerning previous application of the same person, facility, or place specified in the application. (86-293(1), 86-291).

Order:

Order good within the territorial jurisdiction of court. Issuing judge is required to find probable cause that warrants an interception order. The order must specify the (1) identity of the person (if known) whose communications is to be intercepted, (2) the nature/location of the facilities is to be intercepted (unless it's oral interception and the description is not practical or the person is liable to flee), (3) description of the type of communication to be intercepted, (4) identity of the agency authorized to undertake interception; (5) time period and whether interception ends when objective is met. An order may also request assistance of landlord, custodian, or other person to furnish technical assistance to undertake interception. (86-293(3)–(5)).

Order is good for thirty days (unless it states that interception ends when objective communication is first intercepted). Extensions can be made prior to expiration and an application requires all of the above (same information as an initial application). Extension is no longer than practicable but in no case longer than thirty days. (86-293(6)).

Reports:

An issuing judge may require a progress report and, if required, must be submitted between the twelfth and sixteenth day of the interception. If this is required and goes unmet, the judge shall exclude from evidence any communication intercepted after the date authorized in the order unless failure to report is for good cause. (86-293(7)).

The Attorney General and each county attorney annually submit a report to the Administrative Office of the U.S. courts concerning the interceptions requested and authorized during the previous year. Information required in the report is the same required under federal law. (86-294).

PEN REGISTER/TRAP & TRACE DEVICE:

May use a pen register or trap and trace upon a written application and order from the court (immediate interception may

commence during an emergency). The application process for pen registers and trap and traces is generally less burdensome than a wiretap. The application requires: (a) an oath and affirmation; (b) identity of the investigative or law enforcement officer and agency making the application or conducting the investigation; (c) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation. (86-299).

A court is authorized to issue an order if it finds the pen register or trap and trace device is relevant to an ongoing criminal investigation. An order must specify: (a) identity (if known) of the person leasing the telephone line that the pen register or trap and trace device will be attached; (b) identity (if known) of the person subject to the criminal investigation; (c) the number and physical location (if known) of the telephone line that the pen register or trap and trace device will be attached to and, in the case of a trap and trace device, the geographic limitations (if any); (d) a statement of the offense likely to be obtained; (e) statement whether an applicant is to receive technical assistance to accomplish installation (technical assistance from landlord, guardian, etc.). Order is good for sixty days. Extension request requires the same information listed in this section. (86-2,100).

An applicant may also apply for a mobile tracking device, which is good within the jurisdiction of the court or outside of the jurisdiction if the device is installed inside the court's jurisdiction. (86-2,103).

STORED ELECTRONIC COMMUNICATIONS:

A governmental entity must first obtain a warrant to obtain the contents of information stored in an electronic communication service for 180 days or less. The following procedure applies if the content of information has been stored for 180 days or more (or it involves a remote computing service): warrant—if a governmental entity obtains a warrant, no notice is required to the subscriber/customer; or administrative subpoena or court order—if a governmental entity obtains an administrative subpoena or court order, a notice is required to the subscriber/customer. (86-2, 106(1)–(2)).

An applicant wanting access to a communication stored for 180 days or more (or to access remote computing service) must state whether the court should refrain from providing notice for ninety days to the person affected by the order and must show that there is reason to believe that notice will have an adverse result. Adverse result means “endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.” A

April 2003]

STATE WIRETAP LAWS

1063

interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (e) a full and complete statement of the facts concerning all previous applications known to the person authorizing and making the application made to any judge for authorization to intercept communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; (f) where the application is for an extension, a statement setting forth the results thus far obtained from the interception, or an explanation of the failure to obtain results. (179.470(1)).

The judge may request additional testimony or documentary evidence under oath or affirmation. Oral testimony must be reduced to writing. (179.470(2)).

Order:

An order may be entered within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the application that there is probable cause for belief that a person is committing, has committed or is about to commit an enumerated offense, that particular communications concerning that offense will be obtained through such interception, and that the facilities from which, or the place where, the communications are to be intercepted are being used or are about to be used by such person in connection with the commission of such offense or are leased to, listed in the name of, or commonly used by such person. (179.470(3)).

The order shall specify: (a) the identity of the person, if known, whose communications are to be intercepted, (b) the nature and location of the place where or communication facilities to which authority to intercept is granted, the facilities to be used and the means by which such interceptions shall be made, (c) a description of the type of communication sought to be intercepted, and a statement of the offense to which it relates, (d) the identity of the agency authorized to intercept, and of the person authorizing the application, (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (179.475(1)).

An order can only be for thirty days. One thirty-day extension may be granted. (179.475(3)).

Emergency:

Communications may be intercepted without a court order if: (a) the interception or attempted interception is made with the prior

consent of one of the parties to the communication; and (b) an emergency situation exists. A person who makes an emergency interception shall, within seventy-two hours of the interception, make a written application to a justice of the supreme court or district judge for ratification of the interception. The interception will be ratified only if the applicant shows that: (a) an emergency situation existed and it was impractical to obtain a court order before the interception; and (b) the interception otherwise met the above requirements. (200.620).

Reports:

The issuing judge may require reports, at such intervals as he designates, showing progress toward the authorized objective and the need for continued interception. (179.480).

In January of each year, the Attorney General and the district attorney of each county shall report to the Administrative Office of the U.S. Courts the information required to be reported pursuant to 18 U.S.C. § 2519. A copy of the report must be filed with the investigation division of the department of public safety. (179.515(1)).

Every justice of the supreme court or district judge who signs an intercept order shall, within thirty days after the termination of the order, file with the investigation division of the department of public safety a report containing the same information required to be reported pursuant to 18 U.S.C. § 2519. The report must also indicate whether a party to an intercepted wire communication had consented to the interception.

The investigation division of the department of public safety shall, on or before April 30 of each year, compile a report that summarizes and analyzes all reports submitted to the division during the previous year. (179.515(3)).

PEN REGISTER/TRAP & TRACE DEVICE:

District courts may issue orders authorizing their use upon the application of a district attorney, the Attorney General or their deputies, supported by an affidavit of a peace officer. (179.530).

A peace officer is a sheriff of a county, metropolitan police departments and their deputies; investigators, agents, officers and employees of the investigation division of the department of public safety; special investigators employed by the Attorney General or investigators employed by a district attorney who have the powers of peace officers; policemen of cities and towns; and agents of the state gaming control board who are investigating violations of certain statutory subsections. (179.530).

April 2003]

STATE WIRETAP LAWS

1065

STATE: NEW HAMPSHIRE
N.H. REV. STAT. ANN. §§ 570-
A:1 to -B:7; 644:9 (1986)

PARTY CONSENT : All, unless
officer is a party; then, need
Attorney General's authorization
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The Attorney General, deputy Attorney General, or a designated county attorney, may apply to a judge of competent jurisdiction for an intercept order. (570-A:7).

An application shall be in writing upon oath or affirmation and shall include: (a) the identify of the officer making the application and the officer authorizing the application; (b) a statement of the facts and circumstances justifying the order including details about the offense that has been, is being or will be committed, a description of the nature and location of the facilities from which or the place where the communication will be intercepted; a description of the type of communication to be intercepted and the identity of the person, if known, whose communications are to be intercepted; (c) a statement as to whether other investigative procedures have been tried and failed, or appear unlikely to succeed, or appear to dangerous; (d) a statement as to the time period for which interception is required to be maintained, and if the interception should not automatically terminate after the described communication has first been obtained, a description establishing probable cause that additional communications of the same type are required; (e) a statement of the facts of all previous applications known to the individual making and authorizing the application made to any judge involving the same persons, facilities or places specified in the subject application and the action taken by the judge. (570-A:9(I)).

The applicant must provide evidence of the commission of organized crime, homicide, kidnapping, gambling, theft, corrupt practices, child pornography, computer pornography and child exploitation, criminal conduct in violation of the securities or security takeover disclosure laws, robbery, arson, hindering apprehension or prosecution, tampering with witnesses and informants, felonious sexual assault, escape, bail jumping, insurance fraud, dealing in narcotic drugs, marijuana, or other dangerous drugs, hazardous waste violations, or conspiracy to commit any of the foregoing offenses. (570-A:7).

An intercept order may be executed by the investigative or law enforcement officers having responsibility for the investigation. (570-A:7).

Order:

An order will be entered only upon probable cause that a person is, has or will commit an enumerated crime, that communications concerning that offense will be obtained through interception, that the facilities from which, or the place where the communications will be intercepted is leased to, listed in the name of or commonly used by the person alleged to be involved in the commission of the offense. (570-A:9(III)).

An order must identify the person, if known, whose communications are to be intercepted, the nature and location of the communication facilities as to which, or the place where, authority to intercept is granted, a description of the type of communication to be intercepted and the offense to which it relates, the period of time during which such interception is authorized, including a statement as to whether the interception automatically terminated when the described communication is first obtained. (570-A:9(IV)).

An order will be granted for no more than ten days. An extension may be granted for no longer than ten days. (570-A:2(II)(d)).

Emergency:

Oral authorization for an interception may be given and a written memorandum of said determination and its basis shall be made within seventy-two hours thereafter and be kept on file in the office of the Attorney General. (570-A:2(II)(d)).

Reporting:

The judge authorizing the interception may require reports to be filed, at any time he requests, showing that progress has been made toward achievement of the authorized objective. (570-A:9(VI)).

Within thirty days after the expiration of an intercept order or the denial of an order approving an interception, the judge shall report to the Administrative Office of the U.S. Courts: (a) that an order or extension was applied for; (b) the kind of order or extension applied for; (c) the fact that the order or extension was granted as applied for, was modified, or was denied; (d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (e) the offense specified in the order or application, or extension; (f) the identity of the applying investigative or law enforcement officer and agency making the

April 2003]

STATE WIRETAP LAWS

1067

application and the person authorizing the application; and (g) the nature of the facilities from which or the place where communications were to be intercepted. (570-A:10(I)).

In January of each year, each county attorney shall report to the Attorney General who shall report to the Administrative Office of the U.S. Courts: (a) the information required above with respect to each application for an order made during the preceding year; (b) a general description of the interceptions made under such order or extension, including: (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions; (c) the number of arrests resulting from interceptions, and the offenses for which arrests were made; (d) the number of trials resulting from such interceptions; (e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied; (f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interception. (570-A:10(II)).

On or before December 1 of each odd numbered year, the Attorney General shall include in the above-referenced report, a report concerning the number of applications for orders authorizing or approving the interceptions communications and the number of orders and extensions granted or denied during the preceding 2 years. (570-A:10(III)).

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

Only an Attorney General or deputy Attorney General can make an application. The application must be made in writing under oath or equivalent affirmation to a judge of competent jurisdiction and shall include the identity of the attorney for the state making the application and the identity of the law enforcement agency conducting the investigation and a certification that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. (570-B:4).

Order:

A court will enter an order if the Attorney General or deputy Attorney General has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing

criminal investigation. The order will specify: (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (b) the identity, if known, of the person who is the subject of the criminal investigation; (c) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and (d) a statement of the offense to which the information likely to be obtained relates; and shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. (570-B:5(I)-(II)).

An order shall authorize installation and use for no more than sixty days. Extensions may be granted for a period not to exceed sixty days. (570-B:5(III)).

Report:

On or before December 1 of each odd numbered year, the Attorney General shall include in the required report, a report concerning the number of pen register orders and orders for trap and trace devices applied for by the department of justice. (570-B:7).

WIRETAP:

Application:

The Attorney General, county prosecutor or their designee may authorize, in writing, an application to a judge authorizing the interception of communication by the investigative or law enforcement officers or agency having responsibility for an investigation when such interception may provide evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, terroristic threats, violations of Casino Control Act, arson, burglary, theft and related offenses punishable by imprisonment for more than one year, endangering the welfare of a child, escape, forgery and fraudulent practices punishable by imprisonment for more than one year, alteration of motor vehicle identification numbers, unlawful manufacture, purchase, use, or transfer of firearms, unlawful possession or use of destructive devices or explosives, racketeering, leader of organized crime, organized criminal activity directed toward the unlawful transportation, storage, disposal, discharge, release, abandonment or disposition of any harmful, hazardous, toxic, destructive, or polluting substance, or any conspiracy to commit any of the foregoing offenses or which may

provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of these offenses. (2A:156A-8).

An application, in writing upon oath or affirmation, shall state: (a) the authority of the applicant to make such application; (b) the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept is sought and the identity of whoever authorized the application; (c) a statement of the facts relied upon by the applicant, including: (i) the identity of the particular person, if known, committing the offense and whose communications are to be intercepted; (ii) the details as to the offense that has been, is being, or is about to be committed; (iii) the type of communication to be intercepted; and a showing that there is probable cause to believe that such communication will be communicated on the wire or electronic communication facilities involved or at the particular place where the oral communication is to be intercepted; (iv) the character and location of the particular wire or electronic communication facilities involved or the particular place where the oral communication is to be intercepted; (v) a statement of the period of time for which the interception is required to be maintained; if the character of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (vi) a statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ; (d) a statement of the facts concerning all previous applications, known to the individual authorizing and to the individual making the application, made to any court for authorization to intercept a communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application; (e) such additional testimony or documentary evidence in support of the application as the judge may require; and (f) an application need not meet the requirements if: (a) with respect to the application for an interception of an oral communication: (i) the application is approved by the Attorney General or county prosecutor or a person designated to act for such an official and to perform his duties in and during his actual absence or disability; and (ii) the application contains a full and complete statement as to why specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and (iii) the judge finds that such specification is not practical; (b) with respect to the application for an interception of a

wire or electronic communication: (i) the application is approved by the Attorney General or county prosecutor or a person designated to act for such an official and to perform his duties in and during his actual absence or disability; and (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and (iii) the judge finds that such purpose has been adequately shown. (2A:156A-9).

Order:

The judge may enter an order if he or she determines that there is or was probable cause for belief that: (a) the person whose communication is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an enumerated offense; (b) particular communications concerning such offense may be obtained through such interception; (c) normal investigative procedures with respect to such offense have been tried and have failed or appear to be unlikely to succeed if tried or to be too dangerous to employ; (d) the facilities from which, or the place where, the communications are to be intercepted, are or have been used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by, such individual. (2A:156A-10).

The order must specify the investigative or law enforcement officers or agency to be authorized to intercept qualified by training and experience to execute the interception sought. (2A:156A-12).

As part of the consideration of an application in which there is no corroborative evidence offered, the judge shall inquire in camera as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause. (2A:156A-10).

Each intercept order shall state that: (a) the judge is authorized to issue the order; (b) the identity of, or a particular description of, the person, if known, whose communications are to be intercepted; (c) the character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted, or that specification is not practical or that the purpose to thwart interception by changing facilities has been shown; (d) a particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates; (e) the identity of the

April 2003]

STATE WIRETAP LAWS

1071

investigative or law enforcement officers or agency to whom the authority to intercept is given and the identity of whoever authorized the application; (f) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (2A:156A-12).

Orders to provide evidence of racketeering, leader of organized crime or leader of narcotics trafficking network may authorize interception for no more than thirty days and extensions may be granted for additional periods of not more than thirty days, without limitation on the number of extension orders; provided, however, it shall not exceed six months. (2A:156A-12).

An order entered shall not authorize interception for more than twenty days. An extension may be granted for up to two additional ten-day periods. (2A:156A-12).

A request for extension must state facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. (2A:156A-12).

An intercept order may be executed at any point within the jurisdiction of an investigative or law enforcement officer executing the order. (2A:156-12).

Emergency:

Upon informal application by an authorized applicant, a judge may determine there are grounds upon which an order could be issued, and that an emergency situation exists that involves: (a) the investigation of conspiratorial activities of organized crime or (b) immediate danger of death or serious bodily injury to any person, dictating authorization for immediate interception before an application for an order could with due diligence be submitted and acted upon, the judge may grant verbal approval for such interception without an order, conditioned upon the filing, within forty-eight hours, of an application which, if granted, shall recite the verbal approval and be retroactive to the time of such verbal approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for is denied. If no application is made, the content of the intercepted communication shall be treated as having been illegally obtained. (2A:156A-13).

In the event no application is made or an application made pursuant to this section is denied, the court shall require the wire, tape or other recording of the intercepted communication to be delivered to, and sealed by, the court and such evidence shall be retained by the court and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person or as otherwise authorized by court order. (2A:156A-13).

Reports:

Whenever an order authorizing an interception is entered, the order may require reports to be made to the judge at intervals specified therein, who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. (2A:156A-12).

Within thirty days after the expiration of an order or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Director of the courts stating that: (a) an order, extension or renewal was applied for; (b) the kind of order applied for; (c) the order was granted or was denied; (d) the period of the interception authorized, the number and duration of any extensions; (e) the offense specified in the order; (f) the identity of the person authorizing the application and of the investigative or law enforcement officer and agency for whom it was made; and (g) the character of the facilities from which or the place where the communications were to be intercepted. (2A:156A-22).

All judges of the Superior Court authorized to issue intercept orders shall make annual reports on the operation of this act to the Administrative Director of the Courts. The reports by the judges shall contain (a) the number of applications made; (b) the number of orders issued; (c) the effective periods of such orders; (d) the number and duration of any renewals; (e) the crimes in connection with which the conversations were sought; (f) the names of the applicants; and (g) such other and further particulars as may be required. (2A:156A-23).

The Attorney General shall make annual reports to the Administrative Director of the Courts. These reports shall contain (a) the number of applications made; (b) the number of orders issued; (c) the effective periods of such orders; (d) the number and duration of any renewals; (e) the crimes in connection with which the conversations were sought; (f) the name of the applicants; (g) the number of indictments resulting from each application; (h) the crime or crimes which each indictment charges; and (I) the disposition of each indictment. (2A:156A-23).

The Attorney General shall receive and maintain records of all interceptions authorized pursuant the request of an investigative or law enforcement officer or where one is a party and shall include such information in his annual report to the Governor and the Legislature. It shall be the obligation of all law enforcement agencies in the State to file with the Attorney General relevant information. The information on the forms shall include, but not be limited to (a) the name of the investigative or law enforcement officer making the interception; (b) the law enforcement agency employing the officer

April 2003]

STATE WIRETAP LAWS

1073

involved in the interception; (c) the character of the investigation and (d) the results of such activity. (2A:156A-23).

The Attorney General and the county prosecutor shall maintain records of all interceptions authorized by them where consent has been given. Such records shall include the name of the person requesting the authorization, the reasons for the request, and the results of any authorized interception. The Attorney General shall require that such records maintained by county prosecutors be filed with him periodically and he shall report annually to the Governor and Legislature. (2A:156A-23).

The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the Legislature on such aspects of the operation of this act as they respectively deem appropriate including any recommendations they may care to make as to legislative changes or improvements to effectuate the purposes of this act and to assure and protect individual rights. (2A:156A-23).

STORED ELECTRONIC COMMUNICATIONS:

Application:

If a warrant is obtained by a law enforcement agency, that agency, but no other government entity, may require disclosure. Information pertaining to a subscriber or customer may be disclosed. This record shall be disclosed to a law enforcement agency where it has a warrant, the consent of the subscriber or customer or a court order. (2A:156A-29(a)).

A court order for disclosure may be issued by a judge of competent jurisdiction 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 of an electronic communication service or remote computing service is relevant and material to an ongoing criminal investigation. A judge who has issued an order, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on the provider. (2A:156A-29(e)).

A provider of electronic communication service or remote computing service shall disclose to a law enforcement agency the name, address, telephone number or other subscriber number or identity, and length of service provided to a subscriber or customer of such service and the types of services the subscriber or customer utilized, when the law enforcement entity obtains a grand jury or trial subpoena. (2A:156A-29(f)).

Upon the request of a law enforcement agency, a provider of wire or electronic communication service or a remote computing service shall take all necessary steps to preserve, for a period of ninety days, records and other evidence in its possession pending the issuance of a warrant. The preservation period shall be extended for an additional ninety days upon the request of the law enforcement agency. (2A:156A-29(g)).

A law enforcement agency acting under color of law may include in a court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communication sought in order to preserve those communications. Without notifying the subscriber or customer of the court order, the service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, but in no event later than within two business days after receipt by the provider of the court order and shall confirm to the law enforcement agency that the backup copy has been made. (2A:156A-30(a)).

Notice to the subscriber or customer shall be made by the law enforcement agency within three days after receipt of confirmation that the backup copy has been made. (2A:156A-30(a)).

The service provider shall not destroy or permit the destruction of the backup copy until either the delivery of the information or the resolution of all proceedings, including any appeals, concerning the court order, whichever is later. (2A:156A-30(a)).

The service provider shall release the backup copy to the requesting law enforcement agency if, fourteen days after the agency's notice to the subscriber or customer, the provider has not received written notice from the subscriber or customer that the subscriber or customer has filed a motion to vacate the order or the provider has not initiated proceedings to challenge the request of the agency. (2A:156A-30(a)).

Within fourteen days after notice by the law enforcement agency to the subscriber or customer the subscriber or customer may file a motion to vacate the court order, copies to be served upon the agency and written notice of the challenge to be given to the service provider. A motion to vacate a court order shall be filed in the court which issued the order. The motion or application shall contain an affidavit or sworn statement stating that the applicant is a customer of or subscriber to the service from which the contents of electronic communications maintained for the applicant have been sought and shall contain the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this statute. (2A:156A-30(b)).

April 2003]

STATE WIRETAP LAWS

1075

Service shall be made upon the law enforcement agency by delivering or mailing by registered or certified mail the papers to the person, office or department specified in the notice which the customer received. (2A:156A-30(c)).

If the court finds that the subscriber or customer has properly complied, the court shall order the law enforcement agency to file a sworn response, which may be filed in camera if it includes the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the initial allegations and responses, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the agency's response. (2A:156A-30(d)).

If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the law enforcement agency are maintained, or that there is reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought are maintained, and that there is no reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the statute, it shall order the process quashed. (2A:156A-30(e)).

INTERCEPTION OF ELECTRONIC FUNDS TRANSFER:

No government agency shall intercept an electronic fund transfer without first obtaining a court order. (17:16K-5(a)).

A judge, upon consideration of an application, may enter an order, authorizing the interception of an electronic fund transfer, if the court determines on the basis of the facts submitted by the applicant that there is or was probable cause for belief that: (a) the person whose electronic fund transfer is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an offense; (b) particular communications concerning such offense may be obtained through such interception; (c) normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ. To effect an order issued pursuant to this section, the governmental agency shall deliver a true copy of the order to the financial institution which shall promptly carry out the terms of the order under the direct supervision of the

investigative law enforcement officers or agency authorized to intercept the electronic fund transfer. (17:16K-5(b)-(c)).

STATE: NEW JERSEY **PARTY CONSENT:** None
N.J. STAT. ANN. §§ 2A:156A-1 to **LEGISLATION:** None
-34; 17:16K-4 to -6 (West 2000)

CURRENT LAW

WIRETAP:

Application:

The Attorney General, county prosecutor or their designee may authorize, in writing, an application to a judge authorizing the interception of communication by the investigative or law enforcement officers or agency having responsibility for an investigation when such interception may provide evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, terroristic threats, violations of Casino Control Act, arson, burglary, theft and related offenses punishable by imprisonment for more than one year, endangering the welfare of a child, escape, forgery and fraudulent practices punishable by imprisonment for more than one year, alteration of motor vehicle identification numbers, unlawful manufacture, purchase, use, or transfer of firearms, unlawful possession or use of destructive devices or explosives, racketeering, leader of organized crime, organized criminal activity directed toward the unlawful transportation, storage, disposal, discharge, release, abandonment or disposition of any harmful, hazardous, toxic, destructive, or polluting substance, or any conspiracy to commit any of the foregoing offenses or which may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of these offenses. (2A:156A-8).

An application, in writing upon oath or affirmation, shall state: (a) the authority of the applicant to make such application; (b) the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept is sought and the identity of whoever authorized the application; (c) a statement of the facts relied upon by the applicant, including: (i) the identity of the particular person, if known, committing the offense and whose communications are to be intercepted; (ii) the details as to the offense that has been, is being, or is about to be committed; (iii) the type of communication to be intercepted; and a showing that there is probable cause to believe that such communication will be communicated on the wire or electronic communication facilities

April 2003]

STATE WIRETAP LAWS

1077

involved or at the particular place where the oral communication is to be intercepted; (iv) the character and location of the particular wire or electronic communication facilities involved or the particular place where the oral communication is to be intercepted; (v) a statement of the period of time for which the interception is required to be maintained; if the character of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (vi) a statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ; (d) a statement of the facts concerning all previous applications, known to the individual authorizing and to the individual making the application, made to any court for authorization to intercept a communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application; (e) such additional testimony or documentary evidence in support of the application as the judge may require; and (f) an application need not meet the requirements if: (a) with respect to the application for an interception of an oral communication: (i) the application is approved by the Attorney General or county prosecutor or a person designated to act for such an official and to perform his duties in and during his actual absence or disability; and (ii) the application contains a full and complete statement as to why specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and (iii) the judge finds that such specification is not practical; (b) with respect to the application for an interception of a wire or electronic communication: (i) the application is approved by the Attorney General or county prosecutor or a person designated to act for such an official and to perform his duties in and during his actual absence or disability; and (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and (iii) the judge finds that such purpose has been adequately shown. (2A:156A-9).

Order:

The judge may enter an order if he or she determines that there is or was probable cause for belief that: (a) the person whose communication is to be intercepted is engaging or was engaged over a

period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an enumerated offense; (b) particular communications concerning such offense may be obtained through such interception; (c) normal investigative procedures with respect to such offense have been tried and have failed or appear to be unlikely to succeed if tried or to be too dangerous to employ; (d) the facilities from which, or the place where, the communications are to be intercepted, are or have been used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by, such individual. (2A:156A-10).

The order must specify the investigative or law enforcement officers or agency to be authorized to intercept qualified by training and experience to execute the interception sought. (2A:156A-12).

As part of the consideration of an application in which there is no corroborative evidence offered, the judge shall inquire in camera as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause. (2A:156A-10).

Each intercept order shall state that: (a) the judge is authorized to issue the order; (b) the identity of, or a particular description of, the person, if known, whose communications are to be intercepted; (c) the character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted, or that specification is not practical or that the purpose to thwart interception by changing facilities has been shown; (d) a particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates; (e) the identity of the investigative or law enforcement officers or agency to whom the authority to intercept is given and the identity of whoever authorized the application; (f) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (2A:156A-12).

Orders to provide evidence of racketeering, leader of organized crime or leader of narcotics trafficking network may authorize interception for no more than thirty days and extensions may be granted for additional periods of not more than thirty days, without limitation on the number of extension orders; provided, however, it shall not exceed six months. (2A:156A-12).

April 2003]

STATE WIRETAP LAWS

1079

An order entered shall not authorize interception for more than twenty days. An extension may be granted for up to two additional ten-day periods. (2A:156A-12).

A request for extension must state facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. (2A:156A-12).

An intercept order may be executed at any point within the jurisdiction of an investigative or law enforcement officer executing the order. (2A:156-12).

Emergency:

Upon informal application by an authorized applicant, a judge may determine there are grounds upon which an order could be issued, and that an emergency situation exists that involves: (a) the investigation of conspiratorial activities of organized crime or (b) immediate danger of death or serious bodily injury to any person, dictating authorization for immediate interception before an application for an order could with due diligence be submitted and acted upon, the judge may grant verbal approval for such interception without an order, conditioned upon the filing, within 48 hours, of an application which, if granted, shall recite the verbal approval and be retroactive to the time of such verbal approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for is denied. If no application is made, the content of the intercepted communication shall be treated as having been illegally obtained. (2A:156A-13).

In the event no application is made or an application made pursuant to this section is denied, the court shall require the wire, tape or other recording of the intercepted communication to be delivered to, and sealed by, the court and such evidence shall be retained by the court and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person or as otherwise authorized by court order. (2A:156A-13).

Reports:

Whenever an order authorizing an interception is entered, the order may require reports to be made to the judge at intervals specified therein, who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. (2A:156A-12).

Within thirty days after the expiration of an order or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Director of the courts stating that: (a) an order, extension or renewal was applied for; (b) the kind of order applied for; (c) the order was granted or was

denied; (d) the period of the interception authorized, the number and duration of any extensions; (e) the offense specified in the order; (f) the identity of the person authorizing the application and of the investigative or law enforcement officer and agency for whom it was made; and (g) the character of the facilities from which or the place where the communications were to be intercepted. (2A:156A-22).

All judges of the Superior Court authorized to issue intercept orders shall make annual reports on the operation of this act to the Administrative Director of the Courts. The reports by the judges shall contain (a) the number of applications made; (b) the number of orders issued; (c) the effective periods of such orders; (d) the number and duration of any renewals; (e) the crimes in connection with which the conversations were sought; (f) the names of the applicants; and (g) such other and further particulars as may be required. (2A:156A-23).

The Attorney General shall make annual reports to the Administrative Director of the Courts. These reports shall contain (a) the number of applications made; (b) the number of orders issued; (c) the effective periods of such orders; (d) the number and duration of any renewals; (e) the crimes in connection with which the conversations were sought; (f) the name of the applicants; (g) the number of indictments resulting from each application; (h) the crime or crimes which each indictment charges; and (I) the disposition of each indictment. (2A:156A-23).

The Attorney General shall receive and maintain records of all interceptions authorized pursuant the request of an investigative or law enforcement officer or where one is a party and shall include such information in his annual report to the Governor and the Legislature. It shall be the obligation of all law enforcement agencies in the State to file with the Attorney General relevant information. The information on the forms shall include, but not be limited to (a) the name of the investigative or law enforcement officer making the interception; (b) the law enforcement agency employing the officer involved in the interception; (c) the character of the investigation and (d) the results of such activity. (2A:156A-23).

The Attorney General and the county prosecutor shall maintain records of all interceptions authorized by them where consent has been given. Such records shall include the name of the person requesting the authorization, the reasons for the request, and the results of any authorized interception. The Attorney General shall require that such records maintained by county prosecutors be filed with him periodically and he shall report annually to the Governor and Legislature. (2A:156A-23).

The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the Legislature on

April 2003]

STATE WIRETAP LAWS

1081

such aspects of the operation of this act as they respectively deem appropriate including any recommendations they may care to make as to legislative changes or improvements to effectuate the purposes of this act and to assure and protect individual rights. (2A:156A-23).

STORED ELECTRONIC COMMUNICATIONS:*Application:*

If a warrant is obtained by a law enforcement agency, that agency, but no other government entity, may require disclosure. Information pertaining to a subscriber or customer may be disclosed. This record shall be disclosed to a law enforcement agency where it has a warrant, the consent of the subscriber or customer or a court order. (2A:156A-29(a)).

A court order for disclosure may be issued by a judge of competent jurisdiction 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 of an electronic communication service or remote computing service is relevant and material to an ongoing criminal investigation. A judge who has issued an order, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on the provider. (2A:156A-29(e)).

A provider of electronic communication service or remote computing service shall disclose to a law enforcement agency the name, address, telephone number or other subscriber number or identity, and length of service provided to a subscriber or customer of such service and the types of services the subscriber or customer utilized, when the law enforcement entity obtains a grand jury or trial subpoena. (2A:156A-29(f)).

Upon the request of a law enforcement agency, a provider of wire or electronic communication service or a remote computing service shall take all necessary steps to preserve, for a period of ninety days, records and other evidence in its possession pending the issuance of a warrant. The preservation period shall be extended for an additional ninety days upon the request of the law enforcement agency. (2A:156A-29(g)).

A law enforcement agency acting under color of law may include in a court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communication sought in order to preserve those communications. Without notifying the subscriber or customer of the court order, the service provider shall create the backup copy as soon

as practicable, consistent with its regular business practices, but in no event later than within two business days after receipt by the provider of the court order and shall confirm to the law enforcement agency that the backup copy has been made. (2A:156A-30(a)).

Notice to the subscriber or customer shall be made by the law enforcement agency within three days after receipt of confirmation that the backup copy has been made. (2A:156A-30(a)).

The service provider shall not destroy or permit the destruction of the backup copy until either the delivery of the information or the resolution of all proceedings, including any appeals, concerning the court order, whichever is later. (2A:156A-30(a)).

The service provider shall release the backup copy to the requesting law enforcement agency if, fourteen days after the agency's notice to the subscriber or customer, the provider has not received written notice from the subscriber or customer that the subscriber or customer has filed a motion to vacate the order or the provider has not initiated proceedings to challenge the request of the agency. (2A:156A-30(a)).

Within fourteen days after notice by the law enforcement agency to the subscriber or customer the subscriber or customer may file a motion to vacate the court order, copies to be served upon the agency and written notice of the challenge to be given to the service provider. A motion to vacate a court order shall be filed in the court which issued the order. The motion or application shall contain an affidavit or sworn statement stating that the applicant is a customer of or subscriber to the service from which the contents of electronic communications maintained for the applicant have been sought and shall contain the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this statute. (2A:156A-30(b))

Service shall be made upon the law enforcement agency by delivering or mailing by registered or certified mail the papers to the person, office or department specified in the notice which the customer received. (2A:156A-30(c)).

If the court finds that the subscriber or customer has properly complied, the court shall order the law enforcement agency to file a sworn response, which may be filed in camera if it includes the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the initial allegations and responses, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the agency's response. (2A:156A-30(d)).

April 2003]

STATE WIRETAP LAWS

1083

If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the law enforcement agency are maintained, or that there is reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought are maintained, and that there is no reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the statute, it shall order the process quashed. (2A:156A-30(e)).

INTERCEPTION OF ELECTRONIC FUNDS TRANSFER:

No government agency shall intercept an electronic fund transfer without first obtaining a court order. (17:16K-5(a)).

A judge, upon consideration of an application, may enter an order, authorizing the interception of an electronic fund transfer, if the court determines on the basis of the facts submitted by the applicant that there is or was probable cause for belief that: (a) the person whose electronic fund transfer is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an offense; (b) particular communications concerning such offense may be obtained through such interception; (c) normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ. To effect an order issued pursuant to this section, the governmental agency shall deliver a true copy of the order to the financial institution which shall promptly carry out the terms of the order under the direct supervision of the investigative law enforcement officers or agency authorized to intercept the electronic fund transfer. (17:16K-5(b)-(c)).

STATE: NEW MEXICO
N.M. STAT. ANN. §§ 30-12-1 to
-11 (Michie 2002)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

Application may be made by the Attorney General, district attorney, investigative or law enforcement officer. An application by an investigative or law enforcement officer must be authorized by an officer. (30-12-3).

An application shall be in writing upon oath or affirmation and shall include the following: (a) the identify of the officer making the application and the officer authorizing the application; (b) a complete statement of the facts and circumstances justifying the applicant's belief that an order should be issued including details about the offense that has been, is being or will be committed, a particular description of the nature and location of the facilities from which or the place where the communication will be intercepted; a description of the type of communication to be intercepted and the identity of the person, if known whose communications are to be intercepted; (c) a statement as to whether other investigative procedures have been tried and failed, or reasonably appear unlikely to succeed, or appear too dangerous; (d) a statement as to the time period for which interception is required to be maintained, and if the interception should not automatically terminate after the described communication has first been obtained, a description establishing probable cause that additional communications of the same type are required; and (e) a statement of the facts of all previous applications known to that individuals making and authorizing the application made to any judge involving the same persons, facilities or places specified in the subject application and the action taken by the judge.

The judge may require additional information.

Application may be made for the following offenses: murder, kidnapping, extortion, robbery, trafficking, distribution of controlled substances, bribery of a witness or burglary, aggravated burglary, criminal sexual penetration, arson, mayhem, receiving stolen property or commercial gambling if punishable by imprisonment for more than one year or an organized criminal conspiracy to commit any of these crimes.

April 2003]

STATE WIRETAP LAWS

1085

Order:

An order will be entered only if a judge finds probable cause for belief that a person is, has or will commit an enumerated crime, that communications concerning that offense will be obtained through interception, that the facilities from which, or the place where the communications will be intercepted is leased to, listed in the name of or commonly used by the person alleged to be involved in the commission of the offense.

An order must identify the person, if known, whose communications are to be intercepted, the nature and location of the communication facilities as to which, or the place where, authority to intercept is granted, a description of the type of communication to be intercepted and the offense to which it relates, the period of time during which such interception is authorized, including a statement as to whether the interception automatically terminated when the described communication is first obtained.

An order will not be granted for any period longer than necessary, and in no instance for more than thirty days. An extension may be granted for no longer than thirty days.

An application for extension must set forth the results obtained so far or an explanation as to the failure to obtain results. The order granting an extension may require reports to be made to the judge issuing the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception.

STATE: NEW YORK **PARTY CONSENT:** One
N.Y. CRIM. PRO. LAW §§ 700.05–
.70; 705.05–.35; N.Y. PENAL LAW **LEGISLATION:** Yes
§§ 250.00–.35; N.Y. GEN. BUS.
LAW § 395b (Consol. 2002)

CURRENT LAW**WIRETAP:***Application:*

Designated offense means any one or more of the following crimes: A conspiracy or attempt to commit any of the enumerated offenses or: assault, reckless endangerment, promoting a suicide attempt, criminally negligent homicide, manslaughter, murder, abortion, rape, sodomy, sexual abuse, unlawful imprisonment, kidnapping, coercion, criminal trespass, burglary, criminal mischief, criminal tampering, arson, grand larceny, robbery, unlawful use of

secret scientific material, criminal possession of stolen property, trademark counterfeiting, forgery, criminal possession of a forged instrument, criminal possession of forgery devices, falsifying business records, tampering with public records, offering a false instrument for filing, issuing a false certificate, criminal diversion of prescription medications and prescriptions, escape, absconding from temporary release, promoting prison contraband, hindering prosecution, criminal possession of a weapon, manufacture, transport, disposition and defacement of weapons and dangerous instruments and appliances defined as felonies or prohibited use of weapons as defined, relating to firearms and other dangerous weapons, criminal possession of a controlled substance, criminal sale of a controlled substance, criminally possessing a hypodermic instrument, criminal possession or sale of marihuana, promoting gambling, possession of gambling records, possession of a gambling device, commercial bribing, commercial bribe receiving, bribing a labor official, bribe receiving by a labor official, sports bribing and sports bribe receiving, criminal usury, bribery, bribe receiving, bribe giving for public office and bribe receiving for public office, bribing a witness, bribe receiving by a witness, bribing a juror and bribe receiving by a juror, promoting prostitution, riot, criminal anarchy, eavesdropping, any of the acts designated as felonies of the tax law, which section relates to penalties under the tax on cigarettes, any of the acts designated as felonies in of the administrative code of the city of New York, which section relates to penalties under the cigarette tax, scheme to defraud, any of the acts designated as felonies in the general business law or the environmental conservation law, money laundering where the property involved represents or is represented to be the proceeds of specified criminal conduct which itself constitutes a designated offense, stalking, soliciting or providing support for an act of terrorism, making a terroristic threat, crime of terrorism, hindering prosecution of terrorism, falsely reporting an incident, or placing a false bomb.

A justice may issue an eavesdropping or a video surveillance warrant upon application of an applicant who is authorized by law to investigate, prosecute or participate in the prosecution of the particular designated offense which is the subject of the application.

An order may be issued for no more than thirty days. Such period shall begin on the date designated in the warrant as the effective date, which date may be no later than ten days after the warrant is issued.

An application for an eavesdropping or video surveillance warrant must be made to a justice in writing, and must be subscribed and sworn to by an applicant. It must contain: (a) the identity of the applicant and a statement of the applicant's authority to make such

April 2003]

STATE WIRETAP LAWS

1087

application; and (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an eavesdropping or video surveillance warrant should be issued, including (i) a statement of facts establishing probable cause to believe that a particular designated offense has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted or the video surveillance is to be conducted, (iii) a particular description of the type of the communications sought to be intercepted or of the observations sought to be made, and (iv) the identity of the person, if known, committing such designated offense and whose communications are to be intercepted or who is to be the subject of the video surveillance; (c) a statement that such communications or observations are not otherwise legally privileged; (d) a full and complete statement of facts establishing that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ, to obtain the evidence sought; (e) a statement of the period of time for which the eavesdropping or video surveillance is required to be maintained. If the nature of the investigation is such that the authorization for eavesdropping or video surveillance should not automatically terminate when the described type of communication has been first obtained or when the described type of observation has been first made, a particular description of facts establishing probable cause to believe that additional communications or observations of the same type will occur thereafter; and (f) a full and complete statement of the facts concerning all previous applications, known to the applicant, for an eavesdropping or video surveillance warrant involving any of the same persons, facilities or places specified in the application, and the action taken by the justice on each such application. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts stated in the application are derived in whole or part from the statements of persons other than the applicant, the sources of such facts must be either disclosed or described, and the application must contain facts establishing the existence and reliability of the informants or the reliability of the information supplied by them. The application must also state, so far as possible, the basis of the informant's knowledge or belief. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such affidavits may be based either on personal knowledge of the affiant, or

information and belief with the source thereof and the reason therefor specified.

The warrant must be executed by a law enforcement officer who is a member of the law enforcement agency authorized in the warrant to intercept the communications or conduct the video surveillance.

Order:

An eavesdropping or video surveillance warrant may issue only upon application and probable cause to believe that a particularly described person is committing, has committed, or is about to commit a particular designated offense that particular communications concerning such offense will be obtained through eavesdropping, or upon probable cause to believe that particular observations concerning such offense will be obtained through video surveillance that the facilities from which, or the place where, the communications are to be intercepted or the video surveillance is to be conducted, are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person and upon a showing that normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or to be too dangerous to employ.

The warrant must include the following: (1) the name of the applicant, date of issuance, and the subscription and title of the issuing justice, (2) the identity of the person, if known, whose communications are to be intercepted or who is to be the subject of video surveillance; (3) the nature and location of the communications facilities as to which, or the place where, authority to intercept or conduct video surveillance is granted; (4) a particular description of the type of communications sought to be intercepted or of the type of observations to be made, and a statement of the particular designated offense to which it relates (5) the identity of the law enforcement agency authorized to intercept the communications or conduct the video surveillance; and (6) the period of time during which such interception or observation is authorized, including a statement as to whether or not the interception or video surveillance shall automatically terminate when the described communication has been first obtained or the described observation has been first made.

The warrant will be granted for no more than thirty days. An extension may be granted for no more than thirty days.

The warrant will contain an express authorization to make secret entry upon a private place or premises to install an eavesdropping or video surveillance device, if such entry is necessary to execute the warrant.

April 2003]

STATE WIRETAP LAWS

1089

Emergency:

If there is imminent danger of death or serious physical injury and, under the circumstances, it is impractical for the applicant to prepare a written application without risk of such death or injury occurring, an application for an eavesdropping or video surveillance warrant need not be in writing but may be communicated to a justice by telephone, radio or other means of electronic communication. Where such an oral application is made, the applicant must identify himself and the purpose of his communication or observation, after being sworn. The application must otherwise meet the requirements of the law. Upon being advised of the oral application, a justice shall place under oath the applicant and any other person providing information in support of the application. Such oath or oaths and all of the remaining communication must be recorded, either by means of a voice recording device or verbatim stenographic or verbatim longhand notes. If a voice recording device is used or a stenographic record made, the justice must have the record transcribed, certify to the accuracy of the transcription and file the original record and transcription with the court within twenty-four hours of the issuance of a warrant. If longhand notes are taken, the justice shall subscribe a copy and file it with the court within twenty-four hours of the issuance of a warrant. If it finds that an emergency situation exists and that the requirements of the rule have otherwise been satisfied, it may issue a temporary eavesdropping or video surveillance warrant authorizing eavesdropping or video surveillance for a period not to exceed twenty-four hours. The twenty-four hour period may not be extended nor may a temporary warrant be renewed except by written application.

Reports:

A warrant may require reports to be made to the issuing justice showing what progress has been made toward achievement of the authorized objective and the need for continued eavesdropping or video surveillance at such intervals as the justice may require.

Within thirty days after the termination of an eavesdropping warrant or the expiration of an extension order, the issuing or denying justice must submit such report to the Administrative Office of the United States Courts as is required by federal law.

In January of each year, the Attorney General and each district attorney must submit such report to the Administrative Office of the US courts as is required by federal law.

PEN REGISTER/TRAP & TRACE DEVICE:

A justice may issue an order authorizing the use of a pen register or a trap and trace device upon application of an applicant who is authorized by law to investigate, prosecute or participate in the prosecution of the designated crimes which are the subject of the application.

Application:

An order authorizing the use of a pen register or a trap and trace device may issue only: (1) upon an appropriate application; (2) upon a determination that an application sets forth specific, articulable facts, warranting the applicant's reasonable suspicion that an enumerated crime has been, is being, or is about to be committed and demonstrating that the information likely to be obtained by use of a pen register or trap and trace device is or will be relevant to an ongoing criminal investigation of such crime.

An application for an order or an extension of an order authorizing the use of a pen register or a trap and trace device must be made to a justice in writing, and must be subscribed and sworn to by the applicant.

The application must contain: (a) the identity of the applicant and the identity of the law enforcement agency conducting the investigation; (b) a statement of facts and circumstances sufficient to justify the applicant's belief that an order authorizing the use of a pen register or a trap and trace device should be issued, including: (i) a statement of the specific facts on the basis of which the applicant reasonably suspects that the designated crime has been, is being, or is about to be committed and demonstrating that the information likely to be obtained by use of a pen register or a trap and trace device is or will be relevant to an ongoing criminal investigation of such designated offense; (ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (iii) the identity, if known, of the person who is the subject of the criminal investigation; (iv) the number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and (v) a statement of the designated crime or crimes to which the information likely to be obtained by the use of the pen register or trap and trace device relates; (c) a statement of the period of time for which the authorization for the use of a pen register or a trap and trace device is required; and (d) a statement of the facts concerning all previous applications, known to the applicant, for an order authorizing the use

April 2003]

STATE WIRETAP LAWS

1091

of a pen register or a trap and trace device involving any of the same persons or facilities specified in the application, and the action taken by the justice on each such application.

Order:

An order must contain: (a) the name of the applicant, date of issuance, and the subscription and title of the issuing justice; (b) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (c) the identity, if known, of the person who is the subject of the criminal investigation; (d) the number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and (e) a statement of the designated crime(s) to which the information likely to be obtained by the pen register or trap and trace device relates.

An order shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device

An order issued can be issued for a period not to exceed sixty days. Extensions can be issued for no more than sixty days.

STORED ELECTRONIC COMMUNICATIONS:

Included in general wiretap law.

STATE: NORTH CAROLINA **Party Consent :** One
N.C. GEN. STAT. §§ 14-155; 15A- **LEGISLATION:** None
260 to -265; 15A-286 to -298
(2002)

CURRENT LAW

WIRETAP:

Application:

Orders authorizing or approving the interception may be granted when the interception may provide or has provided evidence of the commission of, or any conspiracy to commit: a drug-trafficking violation, a continuing criminal enterprise in violation or may expedite the apprehension of persons indicted for the commission of, or any conspiracy to commit such offenses; any offense that involves the commission of, or any conspiracy to commit, murder, kidnapping,

hostage taking, robbery, extortion, bribery, rape, or any sexual offense, any felony offense against a minor, any felony obstruction of a criminal investigation, any felony offense involving interference with, or harassment or intimidation of, jurors or witnesses or involving assault or threats against any executive or legislative officer or assault with a firearm or other deadly weapon upon governmental officers or employees, any offense involving the manufacture, assembly, possession, storage, transportation, sale, purchase, delivery, or acquisition of weapons of mass death or destruction, the adulteration or misbranding of food, drugs, cosmetics, etc., with the intent to cause serious injury.

Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication must be made in writing upon oath or affirmation to the judicial review panel. Each application must include the following information: (a) the identity of the office requesting the application; (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including: (i) details as to the particular offense that has been, or is being committed; (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; (iii) a particular description of the type of communications sought to be intercepted; and (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter must be added; (e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making adjudication, made to a judicial review panel for authorization to intercept, or for approval of interceptions of wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by that judicial review panel on each such application; (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results; and (g) before acting on the application, the judicial review panel may examine on oath the

April 2003]

STATE WIRETAP LAWS

1093

person requesting the application or any other person who may possess pertinent information, but information other than that contained in the affidavit may not be considered by the panel in determining whether probable cause exists for the issuance of the order unless the information is either recorded or contemporaneously summarized in the record or on the face of the order by the panel.

The head of any municipal, county, or state law enforcement agency or any district attorney may submit a written request to the Attorney General that the Attorney General apply to a judicial review panel for an electronic surveillance order to be executed within the requesting agency's jurisdiction. The written requests shall be on a form approved by the Attorney General and shall provide sufficient information to form the basis for an application for an electronic surveillance order. The head of a law enforcement agency shall also submit a copy of the request to the district attorney, who shall review the request and forward it to the Attorney General along with any comments he may wish to include. The Attorney General is authorized to review the request and decide whether it is appropriate to submit an application to a judicial review panel for an electronic surveillance order. If a request for an application is deemed inappropriate, the Attorney General shall send a signed, written statement to the person submitting the request, and to the district attorney, summarizing the reasons for failing to make an application. If the Attorney General decides to submit an application to a judicial review panel, he shall notify the requesting agency head, the district attorney, and the head of the local law enforcement agency which has the primary responsibility for enforcing the criminal laws in the location in which the majority of the surveillance will take place, if not the same as the requesting agency head, unless the Attorney General has probable cause to believe that the latter notifications should substantially jeopardize the success of the surveillance or the investigation in general. If a judicial review panel grants an order, a copy of such order shall be sent to the requesting agency head and the district attorney, and a summary of the order shall be sent to the head of the local law enforcement agency with primary responsibility for enforcing the criminal laws in the jurisdiction where the surveillance will take place, if not the same as the requesting agency head, unless the judicial review panel finds probable cause to believe that the latter notifications would substantially jeopardize the success of the surveillance or the investigation.

The Attorney General may apply for electronic surveillance orders independent of, or contrary to, the requests of law enforcement agency heads, nor does it limit the discretion of the Attorney General in determining whether an application is appropriate under any given circumstances.

The Attorney General or his designee may, pursuant to 18 U.S.C. § 2516(2), apply to a judicial review panel for an order authorizing or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offenses as to which the application is made, and for enumerated offenses. A judicial review panel shall be composed of such judges as may be assigned by the Chief Justice of the Supreme Court of North Carolina or an Associate Justice acting as the Chief Justice's designee, which shall review applications for electronic surveillance orders and may issue orders valid throughout the State authorizing such surveillance, and which shall submit a report of its decision to the Chief Justice. A judicial review panel may be appointed by the Chief Justice or an Associate Justice acting as the Chief Justice's designee upon the notification of the Attorney General's Office of the intent to apply for an electronic surveillance order.

A judicial review panel is hereby authorized to grant orders valid throughout the State for the interception of wire, oral, or electronic communications. Applications for such orders may be made by the Attorney General or the Attorney General's designee. The Attorney General or the Attorney General's designee in applying for such orders, and a judicial review panel in granting such orders, shall comply with all procedural requirements of 18 U.S.C. § 2518.

No judge who sits as a member of a judicial review panel shall preside at any trial or proceeding resulting from or in any manner related to information gained pursuant to a lawful electronic surveillance order issued by that panel.

Upon application by the Attorney General a judicial review panel may enter an order authorizing an intercept, if the panel determines on the basis of the facts submitted by the applicant that there is probable cause for belief that: (1) an individual is committing, has committed, or is about to commit an enumerated offense; (2) particular communications concerning that offense will be obtained through such interception; and (3) the facilities from which, or the place where, the communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by the individual described.

Order:

Each intercept order must specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and the means by which such interceptions may be made; (c) a particular description of the type of

April 2003]

STATE WIRETAP LAWS

1095

communication sought to be intercepted and a statement of the particular offense to which it relates; (d) the identity of the agency authorized to intercept the communications and of the person requesting the application; and (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception automatically terminates when the described communication has been first obtained.

No intercept order may be for longer than thirty days. An extension may be granted for no longer than thirty days.

Emergency:

The Attorney General or the Attorney General's designee may make emergency applications as provided by 18 U.S.C. § 2518.

Reports:

The Chief Justice of the North Carolina Supreme Court shall receive a report concerning each decision of a judicial review panel.

An order may require reports to be made to the issuing judicial review panel showing that progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports must be made at such intervals as the panel may require.

In January of each year, the Attorney General must report to the Administrative Office of the United States Court the information required to be filed by 18 U.S.C. § 2519 and file a copy of the report with the Administrative Office of the Courts of North Carolina.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

A law enforcement officer may make an application for an order authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or affirmation, to a superior court judge. Such application must include: (a) the identity of the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and (b) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Order:

A superior court judge may enter an order authorizing the installation and use of a pen register or a trap and trace device within the State if the judge finds: (a) that there is reasonable suspicion to

believe that a felony offense, or a Class A1 or Class 1 misdemeanor offense has been committed; (b) that there are reasonable grounds to suspect that the person named or described in the affidavit committed the offense, if that person is known and can be named or described; and (c) that the results of procedures involving pen registers or trap and trace devices will be of material aid in determining whether the person named in the affidavit committed the offense.

An order: (a) shall specify: (i) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (ii) the identity, if known, of the person who is the subject of the criminal investigation; (iii) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and (iv) the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and (b) shall direct, upon request of the applicant, the furnishing of information, facilities, or technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

An order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. An extension may be granted for no more than sixty days.

STORED ELECTRONIC COMMUNICATIONS:

Included in general wiretap law.

STATE: NORTH DAKOTA
N.D. CENT. CODE § 12.1-15-02;
29-29.2-01 to 29-29.3-05; 44.04-18
(2001)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

An application must be made by the Attorney General, Assistant Attorney General, state's attorney or assistant state's attorney. An officer must authorize the application.

An application must be made in writing upon oath or affirmation (affidavit) and demonstrate that there is probable cause and include the following: (a) the identity of the law enforcement officer making the application, and the officer authorizing the application; (b) a

April 2003]

STATE WIRETAP LAWS

1097

complete statement of the facts and circumstances relied upon by the applicant, to justify the belief that an order should be issued, including: details as to the particular offense that has been, is being, or is about to be committed; a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted; a particular description of the type of communication sought to be intercepted; and the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a complete statement as to whether other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried, or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the intercept order should not automatically terminate when the described type of communication has been first obtained, there must be a particular description of the facts establishing probable cause to believe that additional communications of the same type will occur thereafter; and (e) a complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application.

The judge may require additional information.

The application must demonstrate probable cause regarding the commission or attempted commission of a drug offense.

An order may be executed by a investigative or law enforcement officer.

Order:

An order will be entered, within the territorial jurisdiction of the court in which the judge is sitting, only if there is probable cause for belief that a person is, has or will commit an enumerated offense, that communications concerning that offense will be obtained through interception, that the facilities from which, or the place where the communications will be intercepted is leased to, listed in the name of or commonly used by the person alleged to be involved in the offense.

An order must identify the person, if known, whose communications are to be intercepted, the nature and location of the communication facilities as to which, or the place where, authority to intercept is granted, a description of the type of communication to be intercepted and the offense to which it relates, the period of time during which such interception is authorized, including a statement as

to whether the interception automatically terminates when the described communication is first obtained.

An order will not be granted for more than thirty days. Only one thirty day extension will be granted.

An extension request must set forth the results thus far obtained or a reasonable explanation of the failure to obtain those results.

Reports:

The judge authorizing the interception may require reports to be filed, at any time he requests, showing that progress has been made toward achievement of the authorized objective.

A state's attorney shall report annually to the Attorney General information as to the number of applications made for intercept orders; the offense specified in the order or application; the nature of the facilities from which or the place where communications were to be intercepted; the number of persons whose communications were intercepted, the number of arrests resulting from interceptions, and the offenses for which arrests were made; the number of motions to suppress made with respect to such interceptions and the number granted or denied; the number of convictions resulting from the interceptions and the offenses for which the convictions were obtained; and a general assessment of the importance of the interceptions. The state's attorney shall submit the report to the Attorney General by January first of each year. The report must include all orders and applications made, but not in effect, during the preceding year.

PEN REGISTER/TRAP AND TRACE DEVICE:

Application:

An Attorney General, assistant Attorney General, state's attorney or assistant state's attorney, investigative or law enforcement officer may make application, in writing under oath or equivalent affirmation. Such application must include the identity of the applicant and the law enforcement agency conducting the investigation and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Order:

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the applicant has certified to the court that the information likely to be obtained by such installation

April 2003]

STATE WIRETAP LAWS

1099

and use is relevant to an ongoing criminal investigation. The order must specify: (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (b) the identity, if known, of the person who is the subject of the criminal investigation; (c) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and (d) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

The order must direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

An order may authorize installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. Extensions of the order may be granted for no more than sixty days.

STATE: OHIO
OHIO REV. CODE ANN.
§§ 2933.51-.66 (Anderson 2003)

PARTY CONSENT: ONE
LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Offenses for which an intercept order may be obtained include more than forty felonies.

Application:

The prosecuting attorney of the county in which an interception is to take place or in which an interception device is to be installed, or an assistant to the prosecuting attorney of that county who is specifically designated by the prosecuting attorney to exercise authority under this section, may authorize an application for an interception warrant to a judge of the court of common pleas of the county in which the interception is to take place or in which the interception device is to be installed. The authorizing judge does not include one specifically designated as a probate, domestic relations or juvenile judge.

Each application for an interception warrant shall be made in writing upon oath or affirmation to a judge of the court of common pleas of the county in which the interception is to take place or in which the interception device is to be installed, by a person who has

received training that satisfies the minimum standards established by the Attorney General and the peace officer training commission. Each application shall contain all of the following:

1. The names and offices of the applicant and attorney authorizing the application;

2. The identity of the officers or law enforcement agency that will intercept the wire, oral, or electronic communications;

3. A full and complete statement of the objective in seeking the warrant, and a full and complete statement of the facts and circumstances relied on by the applicant to justify the belief that the warrant should be issued, including, but not limited to the following: (a) The details regarding the designated offense that has been, is being, or is about to be committed; (b) The identity of the person, if known, who has committed, is committing, or is about to commit the designated offense and whose communications are to be intercepted and the location at which the communications are sought to be intercepted; (c) A particular description of the nature and location of the facilities from which, or the place at which, the communication is to be intercepted; (d) A particular description of the type of communication sought to be intercepted, and the basis for believing that evidence relating to a designated offense will be obtained through the interception.

4. A statement as to whether the applicant, or the attorney authorizing the application, knows or has reason to know that the communications sought to be intercepted are privileged, the nature of any privilege that exists, and the basis of the knowledge of the applicant or authorizing attorney of the privileged nature of the communications;

5. A statement of the use to which the contents of an intercepted wire, oral, or electronic communication, or the evidence derived from the communication, will be put;

6. A statement of the period of time for which the interception is required to be maintained, and, if the nature of the investigation requires that the authorization for interception not be terminated automatically when the described type of communication first has been intercepted, a particular description of the facts establishing probable cause to believe that additional communications of the same type will occur after the first intercepted communication;

7. A full and complete statement indicating whether other investigative procedures have been tried and have failed to produce the required evidence or indicating the reason that other investigative procedures reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ in order to obtain evidence;

8. A full and complete statement of the particular facts concerning all previous applications known to the applicant or the

April 2003]

STATE WIRETAP LAWS

1101

authorizing attorney that have been made to a judge for authorization to intercept wire, oral, or electronic communications involving any of the persons, facilities, or places specified in the application, and the action of the judge with respect to each previous application;

9. Unless the Attorney General is a subject of the investigation, a written statement, signed by the Attorney General or an Assistant Attorney General designated by the Attorney General, that they have reviewed the application and either agrees or disagrees with the submission of the application to a judge. A disagreement by the Attorney General or Assistant Attorney General does not preclude the making or consideration of an application.

10. If an application for an interception warrant is for an extension of a warrant, the application shall include, in addition to the information and statements specified above, a statement setting forth the results thus far obtained from the interceptions of wire, oral, or electronic communications, or a reasonable explanation of the failure to obtain results from the interceptions.

Order:

A judge may issue an interception warrant if the judge determines, on the basis of the facts submitted by the person who made the application and all affiants, that:

1. There is probable cause to believe that a particular person is committing, has committed, or is about to commit a designated offense;

2. There is probable cause to believe that particular communications concerning the designated offense will be obtained through the interception of wire, oral, or electronic communications;

3. Normal investigative procedures with respect to the designated offense have been tried and have failed or normal investigative procedures with respect to the designated offense reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ in order to obtain evidence;

4. There is probable cause to believe that the communication facilities from which the communications are to be intercepted, or the place at which oral communications are to be intercepted, are being used or are about to be used in connection with the commission of the designated offense or are leased to, listed in the name of, or commonly used by a person who is the subject of the interception warrant;

5. The investigative officer has received training that satisfies the minimum standards established by the Attorney General and the peace officer training commission to intercept the wire, oral, or electronic communication and is able to execute the interception sought;

The warrant is valid at any place if the interception device is installed within the jurisdiction of the judge who issued the warrant and is then moved to another place by persons other than the investigative officers.

An interception warrant shall terminate when the objective of the warrant has been achieved or upon the expiration of thirty days after the date of commencement of the warrant, whichever occurs first, unless an extension is granted as described in this division. The date of commencement of an interception warrant is the day on which an investigative or law enforcement officer first begins to conduct an interception under the warrant, or the day that is ten days after the warrant is issued, whichever is earlier.

Emergency:

A judge may grant an oral order for an interception without a warrant of a wire, oral, or electronic communication, and shall condition the order upon the filing with the judge, within forty-eight hours, of an application for an interception warrant. The judge must place upon the journal of the court an entry into the record regarding the application. The judge may grant the application if:

1. There appears to be grounds upon which an interception warrant could be issued;
2. There is probable cause to believe that an emergency situation exists with respect to the investigation of an offense;
3. There is probable cause to believe that the emergency situation involves an immediate danger of death or serious physical harm that justifies the authorization for immediate interception of a private wire, oral, or electronic communication before an application for an interception warrant could, with due diligence, be submitted to the judge and acted upon;
4. No statement by the Attorney General or their designee is required prior to consideration of the application.

A judge of a court of common pleas may issue an order authorizing or approving the installation and use, within the jurisdiction of the court, of a pen register or a trap and trace device to obtain information in connection with a criminal investigation.

Reports:

Within thirty days after the expiration of a warrant or the denial of an application for a warrant, the issuing judge shall report the following to the Administrative Office of the United States Courts and to the Attorney General:

1. The fact that an application was made for an interception warrant or extension of an interception warrant;

April 2003]

STATE WIRETAP LAWS

1103

2. The kind of interception warrant or extension for which application was made;

3. The fact that the interception warrant or extension was granted as applied for or was denied;

4. The period of interception authorized by the interception warrant, and the number and duration of any extensions of the warrant;

5. The designated offenses specified in the interception warrant, application, or extension;

6. The identity of the person who made the application, any person who executed any accompanying affidavit to an application, and the prosecuting attorney or assistant prosecuting attorney who authorized the application;

7. The nature of the facilities from which, or the place at which, communications are to be intercepted.

In January of each year, the prosecuting attorney of each county shall report to the Administrative Office of the United States courts and to the Attorney General all information that is required to be reported by federal law.

The Attorney General and the Ohio peace officer training commission shall establish a course of training in the legal and technical aspects of wiretapping and electronic surveillance, shall establish regulations that they find necessary and proper for the training program, and shall establish minimum standards for certification and periodic recertification for investigative officers to be eligible to conduct wiretapping or electronic surveillance.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

A law enforcement officer may make an application to a judge of a court of common pleas for an order authorizing the installation and use, within the jurisdiction of the court, of a pen register or a trap and trace device to obtain information in connection with a criminal investigation. The application shall be in writing and shall be under oath or affirmation. Each application shall contain:

1. The name of the law enforcement officer and his agency making the application and conducting the criminal investigation to which the application relates;

2. The name, if known, of the person to whom the telephone or other line to which the pen register or trap and trace device is to be attached is leased or in whose name that telephone or other line is listed;

3. The name, if known, of the person who is the subject of the criminal investigation to which the application relates;

4. The number and, if known, the physical location of the telephone or other line to which the pen register or the trap and trace device is to be attached;

5. A statement of the offense to which the information that is likely to be obtained by the installation and use of the pen register or trap and trace device relates;

6. A certification by the law enforcement officer making the application that the information that is likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation.

Order:

An order for a pen register or a trap and trace device cannot exceed sixty days. The court may grant an extension of the sixty-day period upon application for an order. An extension of an order issued under this division shall be in effect for a period not to exceed sixty days. The court may order further extensions of the sixty-day extended period upon compliance with this division.

STATE: OKLAHOMA **PARTY CONSENT:** One
OKLA. STAT. tit. 13, §§ 176.1–.14, **LEGISLATION:** Yes
177.1–.5 (2002)

CURRENT LAW

WIRETAP:

The Attorney General, upon application by a district attorney, may make application to a presiding judge of the Court of Criminal Appeals an order authorizing the interception of wire, oral or electronic communications by any law enforcement agency of this state or any political subdivision thereof having responsibility for the investigation of the offense as to which the application is made, when such interception may provide evidence of the commission of the offense of murder, the cultivation or manufacture or distribution of narcotic drugs or other controlled dangerous substances, or trafficking in illegal drugs, and any conspiracy to commit these crimes.

When a law enforcement officer, while engaged in intercepting wire, oral or electronic communications in an authorized manner, intercepts wire, oral or electronic communications relating to offenses for which an order or authorization could have been secured or any of the above offenses, which is other than those specified in the order of authorization, the contents thereof and evidence derived therefrom may be disclosed or used when authorized by the judge if they find on

April 2003]

STATE WIRETAP LAWS

1105

subsequent application that the contents were otherwise intercepted in accordance with state law. Such application shall be made as soon as practicable.

Application:

Each intercept application shall be made in writing upon oath or affirmation to a presiding judge of the Court of Criminal Appeals and shall state the authority of the Attorney General to make such application. Each application shall include the following information:

1. The identity of the law enforcement officer initiating the application and the district attorney authorizing the application to the Attorney General;

2. A full and complete statement of the facts and circumstances relied upon by the Attorney General to justify his belief that an order should be issued, including: (a) details as to the particular offense that has been, is being or is about to be committed; (b) a particular description of the nature and location of the facilities from which, or the place where the wire, oral or electronic communications are to be intercepted; (c) a particular description of the type of communications sought to be intercepted; and (d) the identity of the person, if known, committing the offense and whose wire, oral or electronic communications are to be intercepted;

3. A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be either unlikely to succeed if tried or are too dangerous;

4. A statement of the period of time for which the interception is required to be maintained, and, if the nature of the investigation is such that the authorization for interception should not automatically be terminated when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

5. A full and complete statement of the facts concerning: (a) all previous applications made for authorization to intercept wire, oral or electronic communications involving any of the same persons, facilities or places specified in the application; and (b) the action taken on each such application;

6. Any additional information requested by the judge; and

7. When the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain such results.

Order:

The judge may issue an order authorizing the interception of wire, oral or electronic communications within the territorial jurisdiction of the judicial district of the district attorney requesting the order if the judge determines that:

1. There is probable cause for belief that an individual is committing, has committed or is about to commit a particular offense;
2. There is probable cause to believe that particular communications concerning the offense will be obtained through such interception;
3. Normal investigative procedures have been tried and have failed or reasonably appear to be either unlikely to succeed if tried or are too dangerous; or
4. There is probable cause to believe that the facilities from which, or the place where the wire, oral or electronic communications are to be intercepted, are being used by an individual or are about to be used in connection with the commission of such offense or are leased to, listed in the name of or commonly used by such person.

Each intercept order shall specify:

1. The identity of the person, if known, whose communications are to be intercepted;
2. The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
3. A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
4. The identity of the agency authorized to intercept the communications and of the person authorizing the application;
5. The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained; and
6. Upon request of the applicant, direct that a communication common carrier, landlord, custodian or other person shall furnish the applicant as soon as possible all information, facilities and technical assistance necessary to accomplish the interception with a minimum of interference with the services that such carrier, landlord, custodian or person is furnishing to the person whose communications are sought to be intercepted.

No order may authorize the interception of any wire, oral or electronic communication for any period longer than is necessary to achieve the objective of the authorization, or in any event, longer than thirty days.

Extensions of an order may be granted. The period of extension shall be no longer than the judge deems necessary to achieve the

April 2003]

STATE WIRETAP LAWS

1107

purposes for which the extension was granted, and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception and must terminate upon attainment of the authorized objective or within the time authorized as provided by this section.

Reports:

The intercept order may require reports to be made to the Attorney General and the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at such intervals as the issuing judge may require.

Within thirty days after the expiration of an order, or each extension thereof, or the denial of an order approving an interception, the judge shall submit in a written report to the Administrative Director of the Courts the following information:

1. The fact that an order or extension was applied for;
2. The kind of order or extension applied for;
3. The fact that the order or extension was granted as applied for, was modified, or was denied;
4. The period of interceptions authorized by the order, and the number and duration of any extensions of the order;
5. The offense specified in the order or application, or extension of an order;
6. The identity of the law enforcement officer and agency making the request for the application and the district attorney requesting the Attorney General to make the application; and
7. The nature of the facilities from which or the place where communications were to be intercepted.

In January of each year, the Attorney General shall submit in a written report to the Administrative Director of the Courts the following information:

1. Regarding an order or extension: (a) the fact that it was applied for, (b) the kind applied for, (c) the fact that it was granted as applied for, was modified, or was denied, (d) the period of interceptions authorized, and the number and duration of any extensions of the order, (e) the offense specified, (f) the identity of the law enforcement officer and the agency making the request for the application and the district attorney requesting the Attorney General to make the application, and (g) the nature of the facilities from which or the place where communications were to be intercepted;

2. A general description of the interceptions made under such order or extension, including: (a) the approximate nature and frequency of incriminating communications intercepted; (b) the approximate nature and frequency of other communications intercepted; (c) the approximate number of persons whose communications were intercepted; and (d) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

3. The number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

4. The number of trials resulting from such interceptions;

5. The number of motions to suppress made with respect to such interceptions, and the number granted or denied;

6. The number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

7. The information required by paragraphs 2 through 6 with respect to orders or extensions obtained in a preceding calendar year.

PEN REGISTER/TRAP & TRACE DEVICE

Lawful installation and use of a pen register or trap and trace device requires a court order from a court of general criminal jurisdiction of the state, including a magistrate of such a court (i.e., any justice of the Supreme Court or judge of the Court of Criminal Appeals, Court of Appeals or district court, including associate district judges and special judges).

Application:

An officer, attorney or agent of any law enforcement agency, a district attorney or assistant district attorney or the Attorney General or Assistant Attorney General may make application for a pen register or trap and trace order or an extension thereof. Such application shall be in writing, under oath or equivalent affirmation, to a court of general criminal jurisdiction, and shall include:

1. The identity of the person making the application and the identity of the law enforcement agency conducting the investigation; and

2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

April 2003]

STATE WIRETAP LAWS

1109

Order:

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the person making the application has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order issued under this section shall specify:

1. The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached,

2. The identity, if known, of the person who is the subject of the criminal investigation,

3. The number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order, and

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

5. The order shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

An order authorizing the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. Extensions of such an order may be granted, but each period of extension shall be for a period not to exceed sixty days.

An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

1. The order be sealed until otherwise ordered by the court; and

2. The person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

STATE: OREGON**PARTY CONSENT:** OneOR. REV. STAT. §§ 133.723–.739
(2001)**LEGISLATION:** None**CURRENT LAW****WIRETAP:***Application:*

An order for the interception of wire, electronic or oral communications may be issued by any circuit court judge upon written application made upon oath or affirmation of the individual who is the district attorney or a deputy district attorney authorized by the district attorney for the county in which the order is sought. The application shall include:

1. The name of the district attorney or the deputy district attorney making the application and the authority of the district attorney or the deputy district attorney to make the application;

2. The identity of the investigative or law enforcement officer making the application and the officer authorizing the application;

3. A statement demonstrating that there is probable cause to believe that an individual is committing, has committed or is about to commit, a particular felony of murder, kidnapping, arson, robbery, bribery, extortion or other crime dangerous to life and punishable as a felony, or a crime punishable as a felony under ORS 475.992 or 475.995 or as a misdemeanor under ORS 167.007, or any conspiracy to commit any of the foregoing crimes;

4. A statement of the details, if known, of the particular crime alleged under paragraph (c) of this subsection;

5. A particular description of the nature and location of the facilities from which or the place where the wire, electronic or oral communication is to be intercepted, if known;

6. A particular description of the type of wire, electronic or oral communication sought to be intercepted;

7. The identity of the person, if known, suspected of committing the crime and whose wire, electronic or oral communications are to be intercepted;

8. A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or are likely to be too dangerous;

9. A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of wire, electronic or oral

April 2003]

STATE WIRETAP LAWS

1111

communication has been first obtained, a description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

10. A statement as to whether any prior application has been made to intercept wire, electronic or oral communications from the same person and, if such prior application exists, a statement of the current status of that application;

11. Where the application is for the extension of an existing order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results; and

12. Any additional information required by the judge.

Order:

The judge may enter an order authorizing or approving interception of wire, electronic or oral communications within the state if the judge determines on the basis of the facts submitted by the applicant that:

1. There is probable cause for belief that an individual is committing, has committed or is about to commit a particular crime described above;

2. There is probable cause for belief that particular communications concerning that crime will be obtained through such interception;

3. Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or are likely to be too dangerous; and

4. There is probable cause for belief that the facilities from which, or the place where, the wire, electronic or oral communications to be intercepted are being used, or are about to be used, in connection with the commission of that crime are leased to, listed in the name of, or commonly used by the individual suspected.

Each order shall specify:

1. The identity of the person, if known, whose communications are to be intercepted;

2. The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

3. A particular description of the type of communication sought to be intercepted, and a statement of the particular crime to which it relates;

4. The identity of the agency authorized to intercept the communications and of the person authorizing the application;

5. The period of time during which such interception is authorized (up to thirty days, subject to thirty day extension); including a statement as to whether or not the interception shall

automatically terminate when the described communication has been first obtained; and

6. The name of the applicant, date of issuance, and the signature and title of the issuing judge.

Reports:

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

STATE: PENNSYLVANIA
18 PA. CONS. STAT. §§ 5701–75
(2002)

PARTY CONSENT: One
LEGISLATION: Yes

CURRENT LAW

WIRETAP:

The Attorney General or district attorney, or, during the absence or incapacity of the Attorney General or district attorney, a deputy Attorney General designated in writing by the Attorney General or an assistant district attorney designated in writing by the district attorney of the county wherein the interception is to be made, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of certain enumerated offenses, including terroristic threats.

Application:

Each application for an order of authorization to intercept a wire, electronic or oral communication shall be made in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the interception is to be made and shall contain all of the following:

1. A statement of the authority of the applicant to make such application;
2. A statement of the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept a wire, electronic or oral communication is sought;

April 2003]

STATE WIRETAP LAWS

1113

3. A sworn statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application, which shall include:

a) The identity of the particular person, if known, committing the offense and whose communications are to be intercepted;

b) The details as to the particular offense that has been, is being, or is about to be committed;

c) The particular type of communication to be intercepted;

d) A showing that there is probable cause to believe that such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be intercepted;

e) The character and location of the particular wire communication facility involved or the particular place where the oral communication is to be intercepted;

f) A statement of the period of time for which the interception is required to be maintained, and, if the character of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; and

g) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or are too dangerous to employ.

4. Where the application is for the renewal or extension of an order, a particular statement of facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

5. A complete statement of the facts concerning all previous applications, known to the applicant made to any court for authorization to intercept a wire, electronic or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application.

6. A proposed order of authorization for consideration by the judge.

7. Such additional testimony or documentary evidence in support of the application as the judge may require.

Order:

The judge may enter an order authorizing the interception of wire, electronic or oral communications anywhere within the

Commonwealth, if the judge determines on the basis of the facts submitted by the applicant that there is probable cause for belief that all the following conditions exist:

1. The person whose communications are to be intercepted is committing, has or had committed or is about to commit an offense enumerated above;

2. Particular communications concerning such offense may be obtained through such interception;

3. Normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

4. The facility from which, or the place where, the wire, electronic or oral communications are to be intercepted, is, has been, or is about to be used, in connection with the commission of such offense, or is leased to, listed in the name of, or commonly used by, such person;

5. The investigative or law enforcement officers or agency to be authorized to intercept the communications are qualified by training and experience to execute the interception sought, and are certified; and

6. In the case of an application, other than a renewal or extension, for an order to intercept a communication of a person or on a facility which was the subject of a previous order authorizing interception, the application is based upon new evidence or information different from and in addition to the evidence or information offered to support the prior order, regardless of whether such evidence was derived from prior interceptions or from other sources.

As part of the consideration of an application in which there is no corroborative evidence offered, the judge may inquire *in camera* as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause pursuant to this section.

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

1. The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic, or oral communications is given and the name and official identity of the person who made the application;

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

April 2003]

STATE WIRETAP LAWS

1115

3. The character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted;

4. A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates; and

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

No order shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this chapter by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order. In the event the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. No order shall authorize the interception of wire, electronic or oral communications for any period exceeding thirty days. The thirty-day period begins on the day on which the investigative or law enforcement officers or agency first begins to conduct an interception under the order, or ten days after the order is entered, whichever is earlier. Extensions or renewals of such an order may be granted for additional periods of not more than thirty days each. The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

Emergency:

Whenever, upon informal application, a judge determines there are grounds upon which an order could be issued and that an emergency situation exists with respect to the investigation of an enumerated offense, and involving conspiratorial activities characteristic of organized crime or a substantial danger to life or limb, dictating authorization for immediate interception of wire, electronic or oral communications before an application for an order could with due diligence be submitted to him and acted upon, the judge may grant oral approval for such interception without an order, conditioned upon the filing with him, within forty-eight hours thereafter, of an application for an order which, if granted, shall recite the oral approval and be retroactive to the time of such oral approval.

Such interception shall immediately terminate when the communication sought is obtained or when the application for an order is denied, whichever is earlier. In the event no application for an order is made, the content of any wire, electronic or oral communication intercepted shall be treated as having been obtained in violation of the statute.

Mobile Tracking Devices:

Orders for the installation and use of mobile tracking devices may be issued by a court of common pleas. Such orders may authorize the use of mobile tracking devices within the jurisdiction of the court of common pleas, and outside that jurisdiction but within this Commonwealth, if the device is installed within the jurisdiction of the court of common pleas. An order authorizing the use of one or more mobile tracking devices may be issued to an investigative or law enforcement officer upon written application. Each application shall be by written affidavit, signed and sworn to or affirmed before the court of common pleas. The affidavit shall: (a) state the name and department, agency or address of the affiant; (b) identify the vehicles, containers or items to which, in which or on which the mobile tracking device shall be attached or be placed, and the names of the owners or possessors of the vehicles, containers or items; (c) state the jurisdictional area in which the vehicles, containers or items are expected to be found; and (d) provide a statement setting forth all facts and circumstances which provide the applicant with a reasonable suspicion that criminal activity has been, is or will be in progress and that the use of a mobile tracking device will yield information relevant to the investigation of the criminal activity. The court of common pleas shall be notified in writing within seventy-two hours of the time the mobile tracking device has been activated in place on or within the vehicles, containers or items. Authorization for the use of the mobile tracking device may continue for a period of ninety days from the placement of the device. An extension for an additional ninety days may be granted upon good cause shown. Wherever practicable, the mobile tracking device shall be removed after the authorization period expires. If removal is not practicable, monitoring of the mobile tracking device shall cease at the expiration of the authorization order. Movement of the tracking device within an area protected by a reasonable expectation of privacy shall not be monitored absent exigent circumstances or an order supported by probable cause that criminal activity has been, is or will be in progress in the protected area and that the use of a mobile tracking device in the protected area will yield information relevant to the investigation of the criminal activity.

April 2003]

STATE WIRETAP LAWS

1117

PEN REGISTER/TRAP & TRACE DEVICE:*Application:*

The Attorney General or district attorney or their designee may make application for an order or an extension of an order approving the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device, in writing, under oath or equivalent affirmation, to a court of common pleas or to any superior court judge when an application for an order authorizing interception of wire or electronic communications is or has been made for the targeted telephone or another application for interception under this subchapter has been made involving the same investigation. Such application shall include:

1. The identity and authority of the attorney making the application and the identity of the investigative or law enforcement agency conducting the investigation;
2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency; and
3. An affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance or extension of an order.

Order:

An order for a pen register or trap and trace shall specify:

1. That there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted telephone;
2. The identity, if known, of the person to whom is leased or in whose name is listed the targeted telephone, or in the case of the use of a telecommunication identification interception device, the identity, if known, of the person or persons using the targeted telephone;
3. The identity, if known, of the person who is the subject of the criminal investigation;
4. In the use of pen registers and trap and trace devices only, the physical location of the targeted telephone; and
5. A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device or the telecommunication identification interception device relates.

An order shall authorize the installation and use of a pen register, trap and trace device or a telecommunication identification interception device for a period not to exceed thirty days, and may be extended for additional thirty day periods.

Reports:

Whenever an order authorizing an interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at such intervals as the judge may require. Whenever an interception is authorized pursuant to this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the application for order, shall be filed with the court as soon as practicable after the authorized interception is terminated.

Within thirty days after the expiration of an order or an extension or renewal thereof, or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Office of Pennsylvania Courts stating:

1. That an order, extension or renewal was applied for;
2. The kind of order applied for;
3. That the order was granted as applied for, was modified, or was denied;
4. The period of the interceptions authorized by the order, and the number and duration of any extensions or renewals of the order;
5. The offense specified in the order, or extension or renewal of an order;
6. The name and official identity of the person making the application and of the investigative or law enforcement officer and agency for whom it was made; and
7. The character of the facilities from which or the place where the communications were to be intercepted.

All judges who have issued orders pursuant to this title shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts. The reports by the judges shall contain:

1. The number of applications made;
2. The number of orders issued;
3. The effective periods of such orders;
4. The number and duration of any renewals thereof;
5. The crimes in connection with which the orders were sought;
6. The names and official identity of the applicants; and
7. Such other and further particulars as the Administrative Office of Pennsylvania Courts may require.

The Attorney General shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts and to the Judiciary Committees of the Senate and House of Representatives. The reports by the Attorney General

April 2003]

STATE WIRETAP LAWS

1119

shall contain the same information which must be reported pursuant federal law.

Each district attorney shall annually provide to the Attorney General all of the foregoing information with respect to all applications authorized by that district attorney on forms prescribed by the Attorney General.

The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the General Assembly on such aspects of the operation of the state's interception laws as they deem appropriate and make any recommendations they feel desirable as to legislative changes or improvements to effectuate the purposes of this chapter and to assure and protect individual rights.

The Attorney General and the Commissioner of the Pennsylvania State Police shall establish a course of training in the legal and technical aspects of wiretapping and electronic surveillance as allowed or permitted by this subchapter, shall establish such regulations as they find necessary and proper for such training program and shall establish minimum standards for certification and periodic recertification of Commonwealth investigative or law enforcement officers as eligible to conduct wiretapping or electronic surveillance under this chapter. The Pennsylvania State Police shall charge each investigative or law enforcement officer who enrolls in this training program a reasonable enrollment fee to offset the costs of such training.

The Attorney General shall annually report to the Administrative Office of Pennsylvania Courts on the number of orders for pen registers, trap and trace devices and telecommunication identification interception devices applied for by investigative or law enforcement agencies of the Commonwealth or its political subdivisions.

Each district attorney shall annually provide to the Attorney General information on the number of orders for pen registers, trap and trace devices, and telecommunication identification interception devices applied for on forms prescribed by the Attorney General.

STATE: RHODE ISLAND **PARTY CONSENT:** One
R.I. GEN. LAWS §§ 11-35-21; 12- **LEGISLATION:** Yes
5.1-1 to 12-5.1-16; §§ 12-5.2-1 to
12-5.2-5 (2002)

CURRENT LAW

WIRETAP:

Application:

The Attorney General, or an Assistant Attorney General specially designated by the Attorney General, may apply to the presiding justice of the superior court for an order authorizing the interception of any wire, electronic, or oral communications. Each application must be in writing, subscribed and sworn to by the applicant, and must contain:

1. The identity of the officer making the application;
2. A full and complete statement of the facts and circumstances that justify the applicant's belief that an order should be issued, including:
 - (a) Details as to the particular designated offense that has been, is being, or is about to be committed;
 - (b) A particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted;
 - (c) A particular description of the type of communications sought to be intercepted; and
 - (d) The identity of the person, if known, committing the offense and whose communications are to be intercepted;
3. A full and complete statement as to whether or not other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried, or that they are too dangerous;
4. A statement of the period of time for which the interception is required to be maintained (up to thirty days, plus three-day extensions). If the nature of the investigation dictates that the authorization of interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will subsequently occur;
5. A full and complete statement of the facts concerning all previous applications, known to the individual making the application, made to the presiding justice of the superior court for authorization to intercept wire, electronic, or oral communications

April 2003]

STATE WIRETAP LAWS

1121

involving any of the same persons, facilities or places specified in the application, and the action taken by the presiding justice of the superior court on each application;

6. Where the application is for the extension of an order, a statement setting forth the results obtained from the interception to that point, or a reasonable explanation of the failure to obtain the results; and

7. Any additional testimony or documentary evidence requested by the judge.

Order:

The presiding justice may authorize the interception of wire, electronic, or oral communications if he determines that:

1. There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular designated offense;

2. There is probable cause for belief that particular communications concerning that offense will be obtained through the interception;

3. Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried, or are too dangerous;

4. There is probable cause for belief that the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted, are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by the individual.

If the facilities from which a wire, electronic, or oral communication is to be intercepted are public, no order of authorization shall be issued unless the court additionally determines that there is a special need to intercept wire communications over the facilities.

If the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted, are being used, or are about to be used, or are leased to, listed in the name of, or commonly used by, a licensed attorney-at-law, or an ordained minister of the gospel, priest, or rabbi of any denomination, or is a place used primarily for habitation by a husband and wife, no order shall be issued unless the presiding justice of the superior court additionally determines that there is a special need to intercept wire, electronic, or oral communications over those facilities or in those places, and that the interceptions will be conducted in a way that minimizes or eliminates interception of privileged communication between lawyers and clients, clergymen and confidants, or husbands and wives.

Each order authorizing the interception of any wire, electronic, or oral communication shall specify:

1. The identity, or a particular description of the person, if known, whose communications are to be intercepted;
2. The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
3. A particular description of the type of communications sought to be intercepted, and a statement of the particular offense to which they relate;
4. The identity of the agency authorized to intercept the communications; and
5. The period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

No order may authorize the interception of any wire, electronic, or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted and shall be no longer than the justice deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in a way that minimizes the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

An order may be executed pursuant to its terms anywhere in the state by the authorized applicant personally or by another investigative or law enforcement officer designated by him or the presiding justice.

PEN REGISTER/TRAP & TRACE DEVICES:

Application:

The Attorney General, Assistant Attorney General or law enforcement officer may apply in writing under oath or equivalent affirmation, to the presiding justice of the superior court or his or her designee for an order approving the installation, use or extension of a pen register or a trap and trace device, in order to obtain information regarding a designated offense. Such application shall include:

1. The identity of the Attorney General, Assistant Attorney General, or the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and

April 2003]

STATE WIRETAP LAWS

1123

2. A certification by the applicant that the information likely to be obtained is relevant and necessary to an ongoing criminal investigation, that other investigative procedures have been or are being initiated or conducted, and that the request for the issuance of the pen register and/or trap and trace device is necessary to further an ongoing criminal investigation being conducted by that agency.

Order:

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device if it is reasonably satisfied that the information likely to be obtained is relevant and necessary to further an ongoing criminal investigation, and that use of a pen register or trap and trace device is the least intrusive way to obtain that information. Such order shall specify:

1. The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

2. The identity of the person who is the subject of the criminal investigation;

3. The number and physical location of the telephone lines to which the pen register or trap and trace device is to be attached and, in the case if a trap and trace device, the geographic limits of the trap and trace order;

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device is relevant; and

5. Direction, upon the request of the applicant, for the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

An order shall authorize the installation and use of a pen register or a trap and trace device for no longer than sixty days. Extensions of the order may be granted, but shall not exceed sixty days.

Reports:

The intercept order may require reports to be made to the presiding justice who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. These reports shall be made at whatever intervals the justice requires.

On the second Friday of January, of each year, the Attorney General shall submit a report to the General Assembly stating the number of applications made for orders during the previous year and the number of orders issued. In addition, the report shall provide, for each wiretap order and renewal:

1. A breakdown of the effective period of the wiretap;
2. The designation of the offenses for which the wiretap was sought;
3. The number of interceptions made by the wiretap during the reported year;
4. An indication whether any indictments were obtained as a result of those intercepts;
5. An indication, if any motions to suppress were made, whether the motions were granted; and
6. The prosecutorial results, if any, of the wiretap, including the criminal sentences imposed on any individual who pleads or is convicted of a crime in which wiretaps were instituted.

If the wiretap order is a renewal from a previous year, or a case is closed in which a wiretap order had been previously obtained, the report shall list with this information a separate breakdown of the information for prior years. The report shall not include any information on wiretaps which remain in operation at the time the report is filed. This report shall be a public document. The report shall also include the number of pen registers and trap and trace authorized devices.

State: SOUTH CAROLINA **PARTY CONSENT:** All
 S.C. CODE ANN. §§ 16-17-470, **LEGISLATION:** Yes
 -480, 17-29-20 (Law. Co-op. 2002)

CURRENT LAW

Except as noted below, South Carolina lacks a comprehensive statutory system regarding the interception of wire, oral and electronic communications.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

The Attorney General (or its designee), a circuit solicitor (or its designee) of a political subdivision having law enforcement authority, or a law enforcement officer, may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath to the circuit court of the circuit where the political subdivision is located or if on behalf of the State to any circuit court. Such application must include:

1. The identity of the attorney or the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and

April 2003]

STATE WIRETAP LAWS

1125

2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency, and that the applicant has probable cause to believe that a user of the service to which the pen register or trap and trace device is applied is a participant in the criminal activity being investigated.

Order:

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device if it finds that the attorney or the law enforcement officer has certified to the court that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation, and that probable cause exists. An order also must specify:

1. The identity, if known of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

2. The identity, if known, of the person who is the subject of the criminal investigation, and to whom the probable cause requirement applies;

3. The number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

An order must authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days; extensions may be granted, but only for a period not to exceed sixty days.

STATE: SOUTH DAKOTA **PARTY CONSENT:** One
S.D. CODIFIED LAWS §§ 23-35A- **LEGISLATION:** None
1 to 23A-35A-34 (Michie 2002)

CURRENT LAW

WIRETAP:

Application:

An application shall be made in writing and upon the oath or affirmation of the applicant and include:

1. The name and title of the applicant;

2. A full and complete statement of the facts and circumstances relied upon by the applicant, including the supporting oath or affirmation of the investigating peace officer of any police department of the state or any political subdivision thereof, or the investigating sheriff or deputy of any county, to justify his belief that an order should be issued, including:

(a) Details as to the particular crime that has been, is being or is about to be committed;

(b) The identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) A particular description of the type of communications sought to be intercepted;

(d) A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; and

(e) In the case of a telegraphic or telephonic communication, identifying the particular telephone number or telegraph line involved;

3. A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

4. A statement of the period of time for which the interception is required to be maintained (up to thirty days, subject to thirty-day extension). If the nature of the investigation is such that authorization to intercept should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

5. A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

6. Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

Order:

A judge may enter an order authorizing wiretapping or eavesdropping if he determines that:

April 2003]

STATE WIRETAP LAWS

1127

1. There is probable cause to believe that an individual is committing, has committed, or is about to commit a particular crime;

2. There is probable cause to believe that particular communications concerning that offense will be obtained through such interception;

3. Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and

4. There is probable cause to believe that the facilities from which, or the place where, the wire or oral communications are to be used, in connection with the commission of such offense, or are leased to, listed in the name of or commonly used by such person.

Each order authorizing the interception of any wire or oral communication shall specify:

1. The identity of the person, if known, whose communications are to be intercepted;

2. The nature and location of the communications facilities as to which, or the place where authority to intercept is granted;

3. A particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

4. The identity of the agency authorized to intercept the communications, and of the person authorizing the application;

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

6. That the authorization for wiretapping or eavesdropping be executed as soon as practicable; that it be conducted in such a way as to minimize interception of communications not otherwise subject to interception under this section; and that it shall terminate upon attainment of the authorized objective, or on the date specified, whichever comes first.

Reports:

The order may require written reports to be made to the issuing judge at specified intervals showing the progress made toward achieving the authorized objective and the need for continued interception.

PEN REGISTER/TRAP & TRACE DEVICE:

An investigative or law enforcement officer may apply for an order, or an extension of an order, authorizing or approving the installation and use of a pen register or a trap and trace device in writing under oath or equivalent affirmation, to any circuit court

April 2003]

STATE WIRETAP LAWS

1129

to be committed; (ii) the nature and location of where the communication is to be intercepted; (iii) the type of communications sought to be intercepted; and (iv) The identity of all persons, if known, committing the offense and whose communications are to be or may be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed; (d) a statement of the period of time for which the interception is required to be maintained; (e) a full and complete statement of the facts concerning all previous applications known to the individuals authorizing and making the application, made to any judge for authorization to intercept wire, oral or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application; and (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception.

Order:

Upon such application, the judge may enter an *ex parte* order authorizing interception of wire, oral, or electronic communications within the district in which the judge is sitting, (and outside that district but within the state of Tennessee in the case of a mobile interception device) if the judge determines on the basis of the facts submitted by the applicant that: (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular enumerated offense; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed; (d) there is probable cause for belief that the facilities from which, or the place where, the wire, oral or electronic communications are to be intercepted are being used, or about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person; and (e) each order shall specify: (i) the identity of all persons, if known, whose communications are to be or may be intercepted; (ii) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (iii) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (iv) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and (v) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. An order authorizing the

interception of a wire, oral or electronic communication shall direct that a provider of communication service, landlord, custodian, or other person to furnish the applicant with all information, facilities, and technical assistance necessary to accomplish the interception.

No order may authorize or approve the interception of any wire, oral or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension shall contain a provision that the interception shall be executed as soon as practicable, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception.

The contents of any wire, oral, or electronic communication intercepted shall be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral or electronic communication shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, such recordings shall be made sealed under the judge's direction. All recordings shall be treated as confidential and not be open for inspection by members of the public. They shall not be destroyed except upon an order of the issuing judge and in any event shall be kept for ten years. Upon an order of the issuing judge, the contents of any wire, oral, or electronic communication may be unsealed and used while giving testimony, pursuant to certain conditions. Applications made and orders granted shall be treated as confidential and shall not be open for inspection by members of the public. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall be kept for ten years. Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge. Within a reasonable time, but not later than ninety days after the termination of an order of approval, the issuing or denying judge shall cause to be served on the persons named in the order or application, an inventory which shall include notice of: the fact of entry of the order or the application; the date of the entry and the period of authorized interception, or the denial of the application; and the fact that during the period wire, oral, or electronic communications were or were not intercepted. On an *ex parte*

April 2003]

STATE WIRETAP LAWS

1131

showing of good cause to a judge of competent jurisdiction, the serving of the inventory required by this subsection may be postponed for ninety days. At the end of this period, the judge may allow additional ninety-day extensions, but only on further showing of good cause. The contents of any intercepted wire, oral, or electronic communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a state court.

Emergency:

Lawful (a) to protect the rights or property of the provider of that service; (b) to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications if such provider, its officers, employees, or agents, landlord, custodian or other specified person has been provided with a court order signed by the authorizing judge of competent jurisdiction; (c) to intercept a wire, oral or electronic communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to such interception; or (d) to intercept any wire or electronic communication, the transmission of which is causing harmful interference with any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference.

Reports:

Whenever an order authorizing interception is entered, the order shall require that reports be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Reports shall be made at ten-day intervals, with the first report required on the tenth day after the order is entered. In the event of an extension, a new ten-day reporting requirement will begin, with a report required on the tenth day after the extension is granted.

Within thirty days after the expiration of an order, or the denial of an order approving an interception, the issuing or denying judge shall report to the Attorney General and reporter: (a) the fact that an order or extension was applied for; (b) the kind of order or extension applied for; (c) the fact that the order or extension was granted as applied for, was modified, or was denied; (d) the period of interceptions authorized by the order and the number and duration of any extensions of the order; (e) the offense specified in the order or application, or the extension of an order; (f) the identity of the applying investigative or law enforcement officer or agency making the application and the person authorizing the application; and (g)

the nature of the facilities from which, or the place where, communications were to be intercepted.

In January of each year the Attorney General and reporter shall report to the Administrative Office of the United States Courts, and the speaker of the senate and the speaker of the house of representatives: (a) the above information required with respect to each application for an order or extension made during the preceding calendar year; (b) a general description of the interceptions made under such order or extension, including: (i) the approximate nature and frequency of incriminating communications intercepted; (ii) the approximate nature and frequency of other communications intercepted; (iii) the approximate number of persons whose communications were intercepted; and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions; (c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made; (d) the number of trials resulting from such interceptions; (e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied; (f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and the general assessment of the importance of the interceptions; and (g) the above information with respect to orders or extensions obtained in a preceding calendar year.

PEN REGISTER/TRAP & TRACE DEVICE:

Any circuit or criminal court judge may issue a pen register or trap and trace order pursuant to the provisions and requirements of 18 U.S.C. §3123 *et. seq.*

STORED ELECTRONIC COMMUNICATIONS:

“Electronic storage” means: (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. The law does not specifically address laws relating storage of such communications, but it is implicit that such stored communications fall under the statute.

safely install the wiretapping or electronic surveillance or eavesdropping equipment and, if so, a statement as to why such an entry is necessary and proper under the facts of the particular investigation; (f) a full and complete statement of the facts concerning all applications known to the prosecutor making the application that have been previously made to a judge for authorization to intercept wire, oral, or electronic communications involving any of the persons, facilities, or places specified in the application and of the action taken by the judge on each application; and (g) if the application is for the extension of an order, a statement setting forth the results already obtained from the interception or a reasonable explanation of the failure to obtain results.

The judge may, in an *ex parte* hearing in chambers, require additional testimony or documentary evidence in support of the application, and such testimony or documentary evidence shall be preserved as part of the application.

Order:

The presiding judge of the court of criminal appeals shall appoint one district judge from each of the administrative judicial districts of this state to serve at his pleasure as the judge of competent jurisdiction within that administrative judicial district. Each such judge may act on an application for authorization to intercept wire, oral, or electronic communications if the judge is appointed as the judge of competent jurisdiction within the administrative judicial district in which the following is located: (a) the site of: (i) the proposed interception; or (ii) the interception device to be installed or monitored; (b) the communication device to be intercepted; (c) the billing, residential, or business address of the subscriber to the electronic communications service to be intercepted; (d) the headquarters of the law enforcement agency that makes a request for or executes an order authorizing an interception; or (e) the headquarters of the service provider.

If the judge of competent jurisdiction for an administrative judicial district is absent or unable to serve or if exigent circumstances exist, the application may be made to the judge of competent jurisdiction in an adjacent administrative judicial district. Exigent circumstances does not include a denial of a previous application on the same facts and circumstances. To be valid, the application must fully explain the circumstances justifying application.

The judge may enter an *ex parte* order authorizing interception of wire, oral, or electronic communications if the judge determines from the evidence submitted by the applicant that: (a) there is probable cause to believe that a person is committing, has committed, or is about to commit a particular offense; (b) there is probable cause

April 2003]

STATE WIRETAP LAWS

1135

to believe that particular communications concerning that offense will be obtained through the interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed or to be too dangerous if tried; (d) there is probable cause to believe that the facilities from which or the place where the wire, oral, or electronic communications are to be intercepted are being used or are about to be used in connection with the commission of an offense; and (e) a covert entry is or is not necessary to properly and safely install the wiretapping or electronic surveillance or eavesdropping equipment.

An order must specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which or the place where authority to intercept is granted; (c) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates; (d) the identity of the officer making the request and the identity of the prosecutor; (e) the time during which the interception is authorized, including a statement of whether or not the interception will automatically terminate when the described communication is first obtained; and (f) whether or not a covert entry or surreptitious entry is necessary to properly and safely install wiretapping, electronic surveillance, or eavesdropping equipment.

The judge may issue a separate order directing that a provider of wire or electronic communications service or other person furnish the applicant all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively.

An order may not authorize the interception for longer than is necessary to achieve the objective and in no event for more than thirty days. The issuing judge may grant extensions of an order, but only on application for an extension. The period of extension may not be longer than necessary to achieve the purposes for which it is granted and in no event for more than thirty days. Each order and extension must provide that the authorization to intercept be executed as soon as practicable, be conducted in a way that minimizes the interception of communications not otherwise subject to interception, and terminate on obtaining the authorized objective or within thirty days, whichever occurs sooner. If the intercepted communication is in code or a foreign language and an expert in that code or language is not reasonably available during the period of interception, minimization may be accomplished as soon as practicable after the interception.

An order may not authorize a covert entry into a residence solely for the purpose of intercepting a wire or electronic communication.

An order may not authorize a covert entry into or onto a premises for the purpose of intercepting an oral communication unless: (a) the judge determines that: (i) the premises has been the subject of a pen register previously authorized in connection with the same investigation; (ii) the premises which the covert entry is authorized has been the subject of an interception of wire or electronic communications previously authorized in connection with the same investigation; and (iii) that such procedures have failed.

Reports:

Whenever an order authorizing interception is entered, the order may require reports to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. A judge who issues an order authorizing the interception of a wire, oral, or electronic communication may not hear a criminal prosecution in which evidence derived from the interception may be used or in which the order may be an issue.

Within thirty days after the date an order or the last extension, if any, expires or after the denial of an order, the issuing or denying judge shall report to the Administrative Office of the United States Courts: (a) the fact that an order or extension was applied for; (b) the kind of order or extension applied for; (c) the fact that the order or extension was granted as applied for, was modified, or was denied; (d) the period of interceptions authorized by the order and the number and duration of any extensions of the order; (e) the offense specified in the order or application or extension; (f) the identity of the officer making the request and the prosecutor; and (g) the nature of the facilities from which or the place where communications were to be intercepted.

In January of each year each prosecutor shall report to the Administrative Office of the United States Courts the following information for the preceding calendar year: (a) the information required by subsection (a) of this section with respect to each application for an order or extension made; (b) a general description of the interceptions made under each order or extension, including the approximate nature and frequency of incriminating communications intercepted, the approximate nature and frequency of other communications intercepted, the approximate number of persons whose communications were intercepted, and the approximate nature, amount, and cost of the manpower and other resources used in the interceptions; (c) the number of arrests resulting from interceptions made under each order or extension and the offenses for which arrests were made; (d) the number of trials resulting from interceptions; (e) the number of motions to suppress

April 2003]

STATE WIRETAP LAWS

1137

made with respect to interceptions and the number granted or denied; (f) the number of convictions resulting from interceptions, the offenses for which the convictions were obtained, and a general assessment of the importance of the interceptions; and (g) the above information required with respect to orders or extensions obtained.

Any judge or prosecutor required to file a report with the Administrative Office of the United States Courts shall forward a copy of such report to the director of the Department of Public Safety. On or before March 1 of each year, the director shall submit to the governor; lieutenant governor; speaker of the house of representatives; chairman, senate jurisprudence committee; and chairman, house of representatives criminal jurisprudence committee a report of all intercepts as defined herein conducted pursuant to this article and terminated during the preceding calendar year. Such report shall include: (a) the reports of judges and prosecuting attorneys forwarded to the director as required in this section; (b) the number of Department of Public Safety personnel authorized to possess, install, or operate electronic, mechanical, or other devices; (c) the number of Department of Public Safety and other law enforcement personnel who participated or engaged in the seizure of intercepts pursuant to this article during the preceding calendar year; and (d) the total cost to the Department of Public Safety of all activities and procedures relating to the seizure of intercepts during the preceding calendar year, including costs of equipment, manpower, and expenses incurred as compensation for use of facilities or technical assistance provided to the department.

PEN REGISTER/TRAP & TRACE DEVICE:

A person commits an offense if the person knowingly installs or uses a pen register or trap and trace device to record or decode electronic or other impulses for the purpose of identifying telephone numbers dialed or otherwise transmitted on a telephone line. It is an affirmative defense that the actor is: (a) an officer, employee, or agent of a communications common carrier and the actor installs or uses a device or equipment to record a number dialed from or to a telephone instrument in the normal course of business of the carrier for purposes of: (i) protecting property or services provided by the carrier; or (ii) assisting another who the actor reasonably believes to be a peace officer authorized to install or use a pen register or trap and trace device (b) an officer, employee, or agent of a lawful enterprise and the actor installs or uses a device or equipment while engaged in an activity that: (i) is a necessary incident to the rendition of service or to the protection of property of or services provided by the enterprise; and (ii) is not made for the purpose of gathering information for a law enforcement agency or private investigative

agency, other than information related to the theft of communication or information services provided by the enterprise; or (c) a person authorized to install or use a pen register or trap and trace device. An offense under this section is a state jail felony.

STORED ELECTRONIC COMMUNICATIONS:

Electronic storage means a temporary, intermediate storage of a wire or electronic communication that is incidental to the electronic transmission of the communication; or storage of a wire or electronic communication by an electronic communication service for purposes of backup protection of the communication. A person commits an offense if the person obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by: (a) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or (b) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided.

STATE: UTAH

UTAH CODE ANN. §§ 77-23a-4,
-23a-5, -23a-8, -23a-10; 76-9-403
(2002)

PARTY CONSENT: One

LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The Attorney General of the state, any Assistant Attorney General specially designated by Attorney General, any county attorney, district attorney, deputy county attorney, or deputy district attorney specially designated by the county attorney or by the district attorney, may authorize an application to a judge of competent jurisdiction for an order for an interception of wire, electronic, or oral communications by any law enforcement agency of the state, the federal government or of any political subdivision of the state that is responsible for investigating the type of offense for which the application is made. The judge may grant the order in conformity with the required procedures when the interception sought may provide or has provided evidence of the commission of one of several enumerated crimes.

Each application for an order shall be made in writing, upon oath or affirmation to a judge of competent jurisdiction, and shall state the

April 2003]

STATE WIRETAP LAWS

1139

applicant's authority to make the application. Each application shall include:

(a) The identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) A full and complete statement of the facts and circumstances relied upon, including:

(i) Details regarding the particular offense that has been, is being, or is about to be committed;

(ii) A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;

(iii) A particular description of the type of communication sought to be intercepted; and

(iv) The identity of the person, if known, committing the offense and whose communication is to be intercepted;

(c) A full and complete statement as to whether other investigative procedures have been tried and failed or why they reasonably appear to be either unlikely to succeed if tried or too dangerous;

(d) A statement of the period of time for which the interception is required to be maintained;

(e) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and the individual making the application, made to any judge for authorization to intercept, or for approval of interceptions involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each application;

(f) When the application is for the extension of an order, a statement setting forth the results so far obtained from the interception, or a reasonable explanation of the failure to obtain results; and

(g) Additional testimony or documentary evidence in support of the application as the judge may require.

Order:

The judge may enter an *ex parte* order authorizing or approving interception of wire, electronic, or oral communications within the territorial jurisdiction of the state if the judge determines on the basis of the facts submitted by the applicant that:

(a) There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense;

(b) There is probable cause for belief that particular communications concerning that offense will be obtained through the interception;

(c) Normal investigative procedures have been tried and have failed or reasonably appear to be either unlikely to succeed if tried or too dangerous; and

(d) There is probable cause for belief that the facilities from which or the place where the wire, electronic, or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by that person.

Each order shall specify:

(a) The identity of the person, if known, whose communications are to be intercepted;

(b) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) A particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) The identity of the agency authorized to intercept the communications, and of the persons authorizing the application; and

(e) The period of time during which the interception is authorized, including a statement as to whether the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, electronic, or oral communication shall direct that a provider or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference. Any provider or other person furnishing the facilities or technical assistance shall be compensated by the applicant for reasonable expenses.

An order may not authorize or approve the interception for any period longer than is necessary to achieve the objective of the authorization, but in any event for no longer than thirty days.

Extensions of an order may be granted, but only upon application and if the court makes certain findings. The period of extension may be no longer than the authorizing judge considers necessary, but in no event for longer than thirty days.

Every order and extension shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted so as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event within thirty days.

April 2003]

STATE WIRETAP LAWS

1141

Reports:

When an order authorizing interception is entered, the order may require reports to be made to the judge who issued the order, showing what progress has been made toward achievement of the authorized objective and the need for continued interception. These reports shall be made at intervals the judge may require.

Within a reasonable time, but not later than ninety days after the termination of the period of an order or extensions, the judge shall cause serve the persons named in the order or the application an inventory, which shall include notice of:

- (a) The entry of the order or application;
- (b) The date of the entry and the period of authorization, approved or disapproved interception, or the denial of the application; and
- (c) That during the period wire, electronic, or oral communications were or were not intercepted.

Emergency:

Any investigative or law enforcement officer who is specially designated by either the Attorney General, a county attorney or district attorney may intercept wire, electronic, or oral communication if an application for an order approving the interception is made in accordance with this section and within forty-eight hours after the interception has occurred or begins to occur, when the investigative or law enforcement officer reasonably determines that:

- (a) An emergency situation exists that involves:
 - (i) Immediate danger of death or serious physical injury to any person;
 - (ii) Conspiratorial activities threatening the national security interest; or
 - (iii) Conspiratorial activities characteristic of organized crime, that require a wire, electronic, or oral communication to be intercepted before an order authorizing interception can, with diligence, be obtained; and
- (b) There are grounds upon which an order could be entered under this chapter to authorize the interception.

The interception immediately terminates when the communication sought is obtained or when the application for the order is denied, whichever is earlier.

The judge, upon filing of a motion, may in his discretion make available to the person or his counsel for inspection the portions of the intercepted communications, applications, and orders the judge determines to be in the interest of justice.

The contents of any intercepted communication may not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a federal or state court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

1. The Attorney General, a Deputy Attorney General, a county attorney or district attorney, a deputy county attorney or deputy district attorney, or a prosecuting attorney for a political subdivision of the state, or a law enforcement officer, may make application for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device, in writing and under oath or equivalent affirmation, to a court of competent jurisdiction.

2. An application shall include: (a) the identity of the attorney for the government or the law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (b) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Order:

1. In general, upon an application, the court shall enter an *ex parte* order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the attorney for the government or the law enforcement or investigative officer has certified to the court that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.

2. (a) An order issued under this section shall specify: (i) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; (ii) the identity, if known, of the person who is the subject of the criminal investigation; (iii) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographical limits of the trap and trace order; and (iv) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device

April 2003]

STATE WIRETAP LAWS

1143

relates. (b) The order shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

3. An order issued under this section may authorize the installation and use of a pen register or trap and trace device for a period not to exceed sixty days. Extensions of an order may be granted, but only upon an application for an order and upon the judicial finding required by subsection (1). The period of extension shall be for a period not to exceed sixty days.

4. An order authorizing or approving the installation and use of a pen register or trap and trace device shall direct that: (a) the order be sealed until otherwise ordered by the court; and (b) the person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless otherwise ordered by the court.

STATE: VERMONT**PARTY CONSENT:** N/A**LEGISLATION:** Yes**CURRENT LAW**

Vermont lacks a comprehensive statutory system regarding the interception of wire, oral and electronic communications.

STATE: VIRGINIA
VA CODE ANN. §§ 19.2-61 to
19.2-70.3 (Michie 2002)

PARTY CONSENT: One**LEGISLATION:** Yes**CURRENT LAW****WIRETAP:***Application:*

Each application for an order shall be made in writing upon oath or affirmation to the appropriate judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall be verified by the Attorney General to the best of his knowledge and belief and shall include: (a) the identity of the attorney for the Commonwealth and law-enforcement officer who requested the Attorney General to apply for such order; (b) a full and complete statement of the facts and circumstances relied upon

including: (i) details as to the particular offense that has been, is being or is about to be committed; (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; (iii) a particular description of the type of communications sought to be intercepted; and (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained; (e) a full and complete statement of the facts concerning all previous applications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception; and (g) if authorization is requested for observation or monitoring by a police department of a county or city or by law-enforcement officers of the United States, a statement containing the name of the police department or United States agency, and an explanation of the reasons such observation or monitoring is necessary.

Order:

The judge may enter an *ex parte* order authorizing interception within the territorial jurisdiction of the court in which the judge is sitting, and outside that jurisdiction but within the Commonwealth in the case of a mobile interception device, if the judge determines that:

1. There is probable cause for belief that an individual is committing, has committed or is about to commit an offense;
2. There is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
3. Normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or to be too dangerous;
4. There is probable cause for belief that the facilities from which, or the place where, the wire, electronic or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person;
5. A wire, electronic or oral communication shall be deemed to be intercepted in the jurisdiction where the communication is actually intercepted and the monitoring of such intercepted communication may be at any location within the Commonwealth of Virginia.

April 2003]

STATE WIRETAP LAWS

1145

Each order shall specify:

1. The identity of the person, if known, whose communications are to be intercepted;
2. The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
3. A particular description of the type of communication sought to be intercepted, and a statement of the particular specified offense to which it relates;
4. That such interception is to be conducted only by the Department of State Police;
5. If observation or monitoring by the police department of a county or city or by law-enforcement officers of the United States is authorized, only that police department or agency shall observe or monitor the interception; and
6. The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of communication shall direct that a provider of communications or other person shall furnish the Department of State Police forthwith all assistance necessary to accomplish the interception unobtrusively and with a minimum of interference. Any provider of communications or other person furnishing such facilities or technical assistance shall be compensated therefor by the Commonwealth for reasonable and actual expenses incurred in providing such facilities or assistance, to be paid out of the criminal fund.

No order may authorize the interception of any wire, electronic or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

Reports:

Whenever an order authorizing interception is entered, the order shall require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the

authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge shall require.

The courts and the Attorney General must file all reports required by 18 U.S.C. § 2519. By December 31 of each year, the Attorney General must file a written report with the clerks of the Senate and House of Delegates providing the (a) number of applications made, (b) the number of interceptions authorized, (c) the number of arrests resulting from the application, (d) the number of convictions (must provide a breakdown by offense); (e) the cost of each application granted, and (f) the number of requests denied. The clerk must make the information available to any member of the General Assembly.

Within a reasonable time but not later than ninety days after the filing of an application for an order of authorization which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of:

- (a) The fact of the entry of the order or the application;
- (b) The date of the entry and the period of authorized interception, or the denial of the application;
- (c) The fact that during the period wire, electronic or oral communications were or were not intercepted; and
- (d) The fact that unless he files a motion with the court within sixty days after the service of notice upon him, the recordation or resume may be destroyed.

The judge shall make available to such person or his counsel for inspection the intercepted communications, applications and orders. The serving of the inventory required by this subsection may be postponed for additional periods, not to exceed thirty days each, upon the *ex parte* showing of good cause to a judge of competent jurisdiction.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

An investigative or law enforcement officer may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or equivalent affirmation, to a court of competent jurisdiction. The application shall include:

April 2003]

STATE WIRETAP LAWS

1147

1. The identity of the officer making the application and the identity of the law-enforcement agency conducting the investigation; and

2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

The application may include a request that the order require information, facilities and technical assistance necessary to accomplish the installation be furnished.

Order:

Upon application, the court shall enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the investigative or law-enforcement officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

The order shall specify:

1. The identity, if known, of the person in whose name the telephone line to which the pen register or trap and trace device is to be attached is listed or to whom the line is leased;

2. The identity, if known, of the person who is the subject of the criminal investigation;

3. The number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

Installation and use of a pen register or a trap and trace device shall be authorized for a period not to exceed sixty days. Extensions of the order may be granted, but only upon application made and order issued in accordance with this section. The period of an extension shall not exceed sixty days.

An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

1. The order and application be sealed until otherwise ordered by the court;

2. Information, facilities and technical assistance necessary to accomplish the installation be furnished if requested in the application; and

3. The person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence

of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

STORED ELECTRONIC COMMUNICATIONS:

Included in the definition of Wire Communication; accordingly, covered under the general statute.

STATE: WASHINGTON **PARTY CONSENT:** All
WASH. REV. CODE §§ 9.73.030; **LEGISLATION:** Yes
9.73.060; 9.73.090 (2003)

CURRENT LAW

WIRETAP:

Application:

Each application shall be made in writing upon oath or affirmation and shall state:

1. The authority of the applicant to make such application;
2. The identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to record a communication or conversation is sought and the identity of whoever authorized the application;
3. A particular statement of the facts relied upon by the applicant to justify his belief that an authorization should be issued, including:
 - (a) The identity of the particular person, if known, committing the offense and whose communications or conversations are to be recorded;
 - (b) The details as to the particular offense that has been, is being, or is about to be committed;
 - (c) The particular type of communication or conversation to be recorded and a showing that there is probable cause to believe such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be recorded;
 - (d) The character and location of the particular wire communication facilities involved or the particular place where the oral communication is to be recorded;
 - (e) A statement of the period of time for which the recording is required to be maintained;
 - (f) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried

April 2003]

STATE WIRETAP LAWS

1149

and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

4. Where the application is for the renewal or extension of an authorization, a particular statement of facts showing the results thus far obtained from the recording, or a reasonable explanation of the failure to obtain such results;

5. A complete statement of the facts concerning all previous applications made to any court for authorization to record a wire or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each application; and

6. Such additional testimony or documentary evidence in support of the application as the judge may require.

Order:

1. An *ex parte* order for the interception of any communication may be issued by any superior court judge in the state upon verified application of either the state Attorney General or any county prosecuting attorney setting forth fully facts and circumstances upon which the application is based and stating that:

(a) There are reasonable grounds to believe that national security is endangered, that a human life is in danger, that arson is about to be committed, or that a riot is about to be committed;

(b) There are reasonable grounds to believe that evidence will be obtained essential to the protection of national security, the preservation of human life, or the prevention of arson or a riot; and

(c) There are no other means readily available for obtaining such information.

2. Where statements are solely upon the information and belief of the applicant, the grounds for the belief must be given.

3. The applicant must state whether any prior application has been made to obtain such communications on the same instrument or for the same person and if such prior application exists the applicant shall disclose the current status thereof.

4. The application and any order shall identify as fully as possible the particular equipment, lines or location from which the information is to be obtained and the purpose thereof.

5. The court may examine upon oath or affirmation the applicant and any witness the applicant desires to produce or the court requires to be produced.

6. Orders shall be effective for fifteen days, after which period the court which issued the order may upon application of the officer who secured the original order renew or continue the order for an additional period not to exceed fifteen days.

STATE: WEST VIRGINIA **PARTY CONSENT:** One
W. VA. CODE § 62-1D-3 to 62- **LEGISLATION:** Yes
1D-16 (2002)

CURRENT LAW

WIRETAP:

The chief justice of the supreme court of appeals shall, on an annual basis, designate five active circuit court judges to individually hear and rule upon applications for orders authorizing the interception of wire, oral or electronic communications.

Application:

The prosecuting attorney may apply to one of the designated circuit judges an order authorizing the interception of wire, oral or electronic communications when the prosecuting attorney has shown reasonable cause to believe the interception would provide evidence of the commission of an enumerated offenses.

Order:

Each application for an order shall be made only to a designated judge by petition in writing upon oath or affirmation and shall state the applicant's authority to make the application. Each application shall set forth the following:

1. The identity of the member of the department of public safety [West Virginia state police] making the application, and of the officer authorizing the application, who shall be the superintendent of the department of public safety [West Virginia state police];
2. A full and complete statement of the facts and circumstances relied upon to justify his or her belief that an order should be issued, including: (a) details as to the particular offense that has been, is being, or is about to be committed; (b) a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted; (c) a particular description of the type of communications sought to be intercepted; and (d) the identity of the person, if known, committing the offense and whose communications are to be intercepted;
3. A full and complete statement showing that other investigative procedures have been tried and failed and why such procedures reasonably appear to be unlikely to succeed if again attempted or that to do so would be unreasonably dangerous and likely to result in death or injury or the destruction of property;
4. A statement of the period of time for which the interception is required to be maintained.

April 2003]

STATE WIRETAP LAWS

1151

5. A full and complete statement of the facts concerning all previous applications for authorization to intercept wire, oral or electronic communications involving any of the same persons, facilities or places specified in the application and the action taken by the court with respect to each such application; and

6. Where the application is for the extension of an order, a statement setting forth the results obtained pursuant to such order from the interception or a reasonable explanation of the failure to obtain any such results.

The designated judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

The designated judge may enter an *ex parte* order, authorizing interception, if the judge determines on the basis of the evidence and argument presented by the applicant that:

1. There is probable cause to believe that one or more individuals are committing, has committed, or are about to commit one or more of the particular enumerated offenses;

2. There is probable cause for belief that particular communications concerning such offense or offenses will be obtained through the interception;

3. Normal investigative procedures have been tried and have failed and reasonably appear to be unlikely to succeed if attempted again, or that to do so would be unreasonably dangerous and likely to result in death or injury or the destruction of property; and

4. There is probable cause to believe that the facilities from which the communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense.

Each order shall specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates; (d) the identity of members of the department of public safety authorized to intercept the communications and of the person authorizing the applications; and (e) the period of time during which the interception is authorized.

An additional order may be issued directing that a provider of communication service, or other person named in such order, furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference. Any provider of communication service or other person furnishing the facilities or technical assistance shall be reasonably compensated therefor by the applicant for such

services and be reimbursed for the reasonable expenses incurred in providing such facilities or assistance.

An order may authorize the interception of any wire, oral or electronic communication for a period of time that is necessary to achieve the objective of the authorization, not to exceed twenty days. Extensions of an order may be granted, by only upon application for an extension made as provided in subsection (a) of this section and upon the court making the findings required by subsection (c) of this section. The period of extension may be no longer than the designated judge deems necessary to achieve the purposes for which it was granted and, in no event, for longer than twenty days.

Reports:

Whenever an order authorizing the interception of any wire, oral or electronic communication is entered, the order shall require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at the intervals required by such order.

Within sixty days of the termination of the ordered interception of wire, oral or electronic communications, the superintendent of the department of public safety shall provide the designated judge who issued said order a list containing the names and addresses of all persons whose communications were intercepted. Within a reasonable time, but not later than ninety days after the termination of the period specified in an order permitting the interception of any wire, oral or electronic communication or extensions thereof, the designated judge shall cause to be served upon the persons named in the order and such other parties to intercepted communications as the designated judge may determine in his or her discretion. Such written notice shall include: (a) the fact of the entry of the order; (b) the date of the entry and the period of authorized interception; and (c) the fact that during the period wire, oral or electronic communications were or were not intercepted. The service of such notice shall be the sole responsibility of the superintendent of the department of public safety.

PEN REGISTER/TRAP & TRACE DEVICES:

Application:

The prosecuting attorney of any county or any duly appointed special prosecutor may make application for an order or an extension of an order authorizing or approving the installation and use of a pen

April 2003]

STATE WIRETAP LAWS

1153

register or a trap and trace device in writing under oath or affirmation, to the designated judge.

Order:

Upon application made to the court, the designated judge shall enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device if the designated judge finds that the applicant has certified to the court that the information likely to be obtained by such installation and used is relevant to an ongoing criminal investigation.

An order shall relate with specificity: (a) the identity of the person to whom the telephone line to which the pen register or trap and trace device is to be attached is leased or in whose name such telephone is listed; (b) the identity, if known, of the person who is the subject of the criminal investigation; (c) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached; and (d) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

An order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed thirty days. One extension of such thirty-day period may be granted by order of the designated judge upon application.

An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that: (a) the order be sealed until otherwise ordered by the court; and (b) the person owning or leasing the line to which the pen register or a trap and trace device is attached, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

Upon the request of an officer or a law-enforcement agency authorized to install and use a pen register or a trap and trace device, or an attorney acting in behalf of such agency or officer, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law-enforcement officer forthwith all information, facilities and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference.

A provider of a wire or electronic communication service, landlord, custodian or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for services.

No cause of action shall lie against any provider of a wire or electronic communication service, its officers, agents or employees for

providing information, facilities or assistance provided or rendered in accordance with the terms of any court order entered pursuant to this section.

STATE: WISCONSIN
WIS. STAT. §§ 968.27-968.37
(2003)

PARTY CONSENT: One
LEGISLATION: Yes

CURRENT LAW

WIRETAP:

Application:

The Attorney General, together with the district attorney of any county, may approve a request of an investigative or law enforcement officer to apply to the chief judge of the judicial administrative district for the county where the interception is to take place for an order authorizing or approving the interception of wire, electronic or oral communications. The chief judge may grant an order by investigative or law enforcement officers having responsibility for the investigation of the offense for which the application is made. The authorization shall be permitted only if the interception may provide or has provided evidence of the commission of the offense of homicide, felony murder, kidnapping, commercial gambling, bribery, extortion, dealing in controlled substances or controlled substance analogs, a computer crime that is a felony, or any conspiracy to commit any of the foregoing offenses.

Each application shall be made in writing upon oath or affirmation to the court and shall state the applicants authority to make the application and may be upon personal knowledge or information and belief. Each application shall include:

1. The identity of the investigative or law enforcement officer making the application, and the officers authorizing the application;
2. A full and complete statement of the facts and circumstances relied upon by the applicant, including: (a) details of the particular offense; (b) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; (c) a particular description of the type of communications sought to be intercepted; and (d) the identity of the person, if known, committing the offense and whose communications are to be intercepted;
3. A full and complete statement whether or not other investigative procedures have been tried and failed or why they

April 2003]

STATE WIRETAP LAWS

1155

reasonably appear to be unlikely to succeed if tried or to be too dangerous;

4. A statement of the period of time for which the interception is required to be maintained, and if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications for the same type will occur thereafter;

5. A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any court for authorization involving any of the same persons, facilities or places specified in the application, and the action taken by the court on each such application;

6. Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results; and

7. Any additional evidence requested by the judge.

Order:

The court may enter an order authorizing or approving interception of wire, electronic or oral communications, if the court determines that:

1. There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense;

2. There is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

3. Other investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

4. There is probable cause for belief that the facilities from which, or the place where the communications are to be intercepted, are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by the person.

Each order shall specify:

1. The identity of the person, if known, whose communications are to be intercepted;

2. The nature and location of the communications facilities which, or the place where authority to intercept is granted and the means by which such interceptions shall be made;

3. A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;

4. The identity of the agency authorized to intercept the communications and of the person authorizing the application; and

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

No order may authorize or approve the interception of any communication for a period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. The thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event be for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

Reports:

The judge may require reports to be made to the court which issued the intercept order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the court requires.

In January of each year, the department of justice shall report to the Administrative Office of the United States Courts such information as is required to be filed under federal law. A duplicate copy of the reports shall be filed, at the same time, with the office of the director of state courts.

PEN REGISTER/TRAP & TRACE DEVICE:

Application:

The Attorney General or a district attorney may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or equivalent affirmation, to a circuit

April 2003]

STATE WIRETAP LAWS

1157

court for the county where the device is to be located. Such application shall include:

1. The identity of the person making the application and the identity of the law enforcement agency conducting the investigation; and
2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Order:

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the applicant has certified to the court that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation. An order shall:

1. Specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;
2. Specify the identity, if known, of the person who is the subject of the criminal investigation;
3. Specify the number and, if known, the physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order;
4. Provide a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
5. Direct, upon the request of the applicant, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device.

An order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. Extensions of the order may be granted, but for a period not to exceed sixty days.

STATE: WYOMING
WYO. STAT. ANN. §§ 7-3-701 to
-712, §§ 7-3-801 to -806 (Michie
2002)

PARTY CONSENT: One
LEGISLATION: None

CURRENT LAW

WIRETAP:

Application:

The Attorney General or the district attorney within whose jurisdiction the order is sought in conjunction with the Attorney General, may authorize an application to a district court judge for an order authorizing the interception of wire, oral or electronic communications by the Wyoming division of criminal investigation, federal criminal law enforcement agency or any law enforcement agency of the state having responsibility for investigation of the offense for which the application is made, if the interception may provide evidence of an attempt to commit, conspiracy to commit, solicitation to commit or the commission of certain designated felony offenses or comparable crimes in any other jurisdiction.

Each application for an order authorizing the interception of wire, oral or electronic communications shall be made in writing upon oath or affirmation to a district court judge and shall state the applicant's authority to make the application. Each application shall include:

1. The identity of the peace officer making the application and of the officer authorizing the application;
2. A full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued, including:
 - (a) Specific facts concerning the particular offense that is being investigated;
 - (b) Except as provided below, a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted;
 - (c) A particular description of the type of communication sought to be intercepted; and
 - (d) The identity of the person or persons, if known, who are suspected of committing the offense and whose communications are to be intercepted;
3. A full and complete statement as to whether or not other investigative procedures have been tried and have failed, or why they reasonably appear to be unlikely to succeed or would be too dangerous;

April 2003]

STATE WIRETAP LAWS

1159

4. A statement of the required duration of the interception (up to thirty days, subject to thirty day extension). If the nature of the investigation will require that the interception not automatically terminate when the described type of communication has been first obtained, the application shall state a particular description of facts sufficient to establish probable cause to believe that additional communications of the same type will occur after the initial interception;

5. A full and complete statement by the applicant concerning all previous applications known to the individual authorizing and making the application to have been made to any judge for permission to intercept wire, oral or electronic communications involving any of the same persons, facilities or places specified in the application, and action taken by the judge on each previous application;

6. If the application is for extension of an order, a complete statement shall be made setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain any results; and

7. Any additional testimony or documentary evidence in support of the application required by the judge.

Order:

The judge may issue an order authorizing interception of wire, oral or electronic communications within the territorial jurisdiction of the court in which the judge is sitting, and outside that jurisdiction but within the state of Wyoming in the case of a mobile interception device authorized by a district court within such district, if the judge determines:

1. There is probable cause for belief that the named person is committing or has committed certain offenses;

2. There is probable cause for belief that particular communications concerning those offenses will be intercepted;

3. Normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed or would be too dangerous; and

4. Except as provided, there is probable cause for belief that the facilities from which, or the place where, the wire, oral or electronic communications are to be intercepted is or is about to be used in connection with an offense or is leased to, listed in the name of or used by the person suspected in the commission of an offense.

Each order shall specify:

1. The identity of the person or persons, if known, whose communications are to be intercepted;

2. The nature and location of the communications facilities as to which, or place where the authority to intercept is granted;

3. A particular description of the type of communication sought to be intercepted and a statement of the particular offense or offenses to which it relates;

4. The period of time during which an interception is authorized including a statement as to whether or not the interception shall automatically terminate when the described communication is first obtained; and

5. The identity of the agency authorized to intercept the communications and of the person authorizing the application.

No order entered may authorize the interception of any wire, oral or electronic communication for any period longer than is necessary to achieve the objective of the authorization, or in any event no longer than thirty days. The thirty day period begins on the earlier of the day on which the peace officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in any event no longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, and that the execution of the permission shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this act. Every order or extension thereof shall also provide that the interception terminate upon attainment of the objective, or in any event in thirty days.

The application need not specify the facilities from which, or the place where, the communication is to be intercepted if:

1. In the case of an application with respect to the interception of an oral communication, the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted and the judge finds that such specification is not practical.

2. In the case of an application with respect to a wire or electronic communication, the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility; the judge finds that such showing has been adequately made; and the order authorizing the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

April 2003]

STATE WIRETAP LAWS

1161

PEN REGISTER/TRAP & TRACE DEVICES:

An attorney for the state may make application for an order or an extension of an order authorizing the installation and use of a pen register or a trap and trace device, in writing under oath or equivalent affirmation, to a district court judge only for investigations of violations of the Wyoming Controlled Substances Act of 1971. Such application shall include:

1. The identity of the attorney making the application and the identity of the law enforcement agency conducting the investigation; and

2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing investigation of a violation of the Wyoming Controlled Substances Act of 1971 being conducted by that agency.

The court shall enter an order authorizing the installation and use of a pen register or a trap and trace device within the state if it finds that the attorney has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing investigation of a violation of the Wyoming Controlled Substances Act of 1971. An order shall state:

1. The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

2. The identity, if known, of the person who is the subject of the criminal investigation;

3. The number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

The order shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. Extensions of the order may be granted, but only for a period not to exceed sixty days.

Reports:

Whenever an order authorizing interception is entered, the order may require reports to be made to the judge issuing the order, stating the progress which has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at intervals as the judge may require.

Upon final execution of an order of interception, the executing agency shall furnish the following information within ten working days to the Attorney General:

1. The fact that an order or extension was applied for, information as to the number of orders, extensions and expansions made by the court including:

(a) Whether or not the order was one that specified the facilities to be used for the interception;

(b) The fact that the order or extension was granted as applied for, was modified or was denied;

(c) The period of interceptions authorized by the order, and the number and duration of any extensions of the order; and

(d) The identity of the applying peace officer and agency making the application and the person authorizing the application.

2. Each offense specified in the application order or extension of an order;

3. The nature of the facilities from which or the place where communications were to be intercepted;

4. A general description of the interceptions made under any order or extension, including the approximate nature and frequency of incriminating communications intercepted and approximate nature and frequency of other communications intercepted, the number of persons whose communications were intercepted and the nature, amount and cost of the manpower and other resources used in the interceptions.

The prosecuting authority or investigating law enforcement agency shall report to the Attorney General by April 1, for the preceding calendar year in which an order was applied for:

1. The number of arrests resulting from interceptions made under the order or extension and the offenses for which arrests were made;

2. The number of trials resulting from such interceptions;

3. The number of motions to suppress made with respect to such interceptions, and the number granted or denied; and

4. The number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions.

The Attorney General shall report to the joint judiciary interim committee no later than July 1 of each year. The report shall contain the information required above.

The Attorney General and Wyoming courts shall report to the Administrative Office of the United States Courts pursuant to federal law.

The Attorney General shall annually report no later than July 1 of each year to the joint judiciary interim committee on the number of pen register orders and orders for trap and trace devices applied for.
