Model Wiretapping & Electronic Surveillance Control Act

Table of Contents

Model Wiretapping & Electronic Surveillance Control Act

Policy Statement

An effective and efficient drug control strategy requires law enforcement to target its resources on the middle and upper echelon participants in the illegal drug distribution network. In order to reach these individuals, it is vitally important for each state to entrust its law enforcement community with the legal tools necessary to implement an effective drug control strategy. One of those tools is court ordered electronic surveillance.

The highest ranking members of drug trafficking conspiracies, as is the case in virtually all organized crime groups, are the most culpable offenders. They are motivated principally, if not exclusively, by greed. They are usually highly sophisticated entrepreneurs who are insulated within the bureaucratic layers of the drug trafficking conspiracy. Consequently, many of our traditional enforcement strategies simply cannot reach these more sophisticated offenders. Experience instructs that the way to cripple drug trafficking and other organized crime is the use of electronic surveillance.

The flow of money to these criminal organizations is incredible, and consequently they have the ability to purchase the latest and most sophisticated technological advances in all fields, including communications. Unless law enforcement agencies are given the most modern tools possible, they will never be able to keep pace with the sophisticated technology available to organized criminal conspiracies.

Court ordered electronic surveillance is a critical weapon in any effort to apprehend and prosecute major narcotics traffickers. For example, in Illinois, electronic surveillance enabled agents of the Northeastern Metropolitan Enforcement Group and the Cook County State's Attorney's Office to infiltrate and dismantle a multi-level conspiracy responsible for the sale of 150 kilograms of cocaine a month in the southern metropolitan Chicago area. The investigation culminated in a 45 day wiretap that targeted land based and cellular telephones listed to a nightclub and a limousine service which were used as fronts by the ringleader of the cocaine organization. Prior to the institution of the wiretap, conventional law enforcement techniques were only able to penetrate middle level street dealers. The wiretap quickly revealed that the drug kingpin had insulated himself with a sophisticated distribution structure consisting of 4 levels and 21 conspirators. As a result of the wiretap, law enforcement officials were able to seize a substantial amount of cocaine, identify organizational sources of cocaine, seize laundered assets and return a 58 count indictment charging all 21 members of the cocaine organization with various mandatory imprisonment violations of the Illinois Controlled Substances Act. All persons charged were convicted; the ringleader was

convicted after he escaped from the county jail and became the first person to be successfully extradited from the country of Turkey to the United States.

Despite the effectiveness of sophisticated electronic surveillance, it is still used sparingly. Although 37 states, the U.S. government, the District of Columbia, Puerto Rico and the Virgin Islands all have some type of electronic surveillance statutes, on average, less than 750 intercepts took place, per year, nationwide, from 1982 through 1991. Since this statute, like all other intercept statutes, has such detailed judicial safeguards and because intercepts are usually highly labor intensive and costly, law enforcement has used them in only the most important and difficult cases. Consequently, this is precisely why we have not seen any of the feared abuses claimed by detractors since the U.S. Congress first adopted a broad based intercept statute in 1968.

The Model Wiretapping and Electronic Surveillance Control Act is based on federal law and seeks to combine effective access to this tool and appropriate safeguards. It permits law enforcement to intercept telephone calls, place electronic "bugs" in locations likely to be used in these conspiracies or to place "body wires" on informants. It also allows access to electronic communications such as facsimile, "beeper" and computer to computer transmissions. The Act permits "roving taps" so that law enforcement can follow a conspirator from public phone to public phone, a technique now used to defeat law enforcement efforts. It permits emergency orders in cases of immediate danger of death or serious injury (i.e., kidnapping). With a court approved warrant, law enforcement agencies will be able to access stored electronic communications or acquire a duplicate pager system to monitor a drug dealer's transactions.

Highlights of the Model Wiretapping & Electronic Surveillance Control Act

REMEDIAL GOAL

- Permits law enforcement authorities, subject to court authorization, to intercept any wire, oral or electronic communication that is being conducted to further certain criminal activity.

PROCEDURES

- Permits, subject to court approval, the use of pen register or trap and trace devices as investigative tools, for short, definitive periods of time.
- Provides for the interception of wire, oral or electronic communications, based on court findings of probable cause, for short, definitive periods of time.
- Allows law enforcement to adapt to all new technologies, as they arise, so that law enforcement's ability to intercept cannot be thwarted either by new technology or new criminal techniques.
- Provides for emergency, oral orders, upon a showing of immediate danger of death or serious injury (i.e., kidnapping).

SAFEGUARDS AND PENALTIES

- Requires court authorization for the use of any pen register, trap and trace or interception device.
- Sets time limitations for the use of any of these devices.
- Requires that law enforcement "minimize" its intercepts, so that only pertinent, relevant information is intercepted.
- Requires that whenever possible, tapes be made of any and all intercepted material for future scrutiny by the court and counsel for the intercepted party.
- Prohibits the use, in any proceeding, of any improperly intercepted information or the fruits thereof.
- Requires the attorney general to report regularly to the office of the courts and to the legislature the number and types of interception authorizations that were sought and the results thereof.
- Provides for civil and criminal penalties and damages for the unlawful interception of communications and the disclosure of any interception orders or the results thereof.

Model Wiretapping & Electronic Surveillance Control Act

Section 1. Short Title.

This [Act] shall be known and may be cited as the "Model Wiretapping and Electronic Surveillance Control Act."

Section 2. Legislative Findings.

(a) The legislature finds that the nation's various telecommunications systems are often used in the furtherance of serious and sometimes violent criminal activities including organized crime, drug trafficking, kidnaping, murder and extortion.

(b) One of the most important and effective tools in the investigation of these crimes by federal, state and local law enforcement agencies is court authorized interception of communications.

(c) Advanced cellular technology, new digital features and new forms of electronic communications have been and will be able to frustrate court orders unless law enforcement officials are given the right to intercept all forms of wire, electronic and oral communications.

(d) In 1968, the Congress of the United States carefully considered and passed the Omnibus Crime Control and Safe Streets Act which laid out a meticulous procedure by which law enforcement can obtain judicial authorization to conduct electronic surveillance. This law was enacted after Congress exhaustively debated the government's need to effectively address serious and often violent criminal conduct against an individual's right to privacy. Nothing in this [Act] needs to change or enhance this authority or procedure.

(e) It is the obligation of state legislatures to provide law enforcement agencies with the appropriate tools with which to keep pace with modern technology. The world of communications is changing with incredible speed and criminals are all too quick to seize every possible advantage. This [Act] provides law enforcement with the speed and flexibility to keep pace with new technology and criminal techniques, while protecting individual privacy rights.

COMMENT

Legislative findings are useful in providing guidance to interpreting courts and publicizing and memorializing the goals and objectives of the [Act]. *Block v. Hirsch*, 256 U.S. 135, 154 (1921) ("entitled at least to great respect").

Unfortunately, the positive advantages gained from advanced telecommunications technology are tempered by the use of such technology to further criminal activities. Court-authorized interceptions of communications are the best weapons to combat illegal activities. However, interceptions that comply with court orders are becoming increasingly difficult with the advent of advanced cellular, digital, electronic, and wire technology.

States have the responsibility of keeping law enforcement agencies effective. Thus, the states have an obligation to provide those agencies with state of the art investigative and surveillance tools that will not only aid law enforcement, but also will protect individual privacy rights.

Section 3. Purpose.

The purpose of this [Act] is to provide a procedure for law enforcement agencies to seek court-approved wire and surveillance orders that will keep pace with modern technology and criminal techniques, while at the same time protecting individual rights and privacy.

COMMENT

This [Act] creates a modern law that encompasses the broad spectrum of wire and electronic surveillance technology to enable state and local law enforcement agencies to pursue all levels of criminal activity with the most sophisticated technology available without infringing on individual privacy and individual rights.

Section 4. Definitions.

As used in this [Act]:

(a) "Aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.

(c) "Attorney for the state" means the attorney general or [appropriate reference, i.e., district attorney, county attorney, etc.] authorized to commence and prosecute an action under this [Act].

(c) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

(d) "Communication common carrier" shall have the same meaning which is given the term "common carrier" by 47 U.S.C. §153(h).

(e) "Contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purpose, or meaning of that communication.

(f) "Court of competent jurisdiction" means a court of general criminal jurisdiction of this state.

(g) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects intrastate, interstate or foreign commerce, excluding:

(1) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(2) any wire or oral communication;

(3) any communication made through a tone only paging device; or

(4) any communication from a tracking device.

(h) "Electronic communication service" means any service which provides to its users the ability to send or receive wire or electronic communications.

(i) "Electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(j) "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:

(1) any telephone or telegraph instrument, equipment or facility, or any component thereof:

(A) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business, and being used by the subscriber or user in the ordinary course of its business, or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(B) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of the officer's duties; or

(2) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(k) "Electronic storage" means:

(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 back-up protection of such communication.

(l) "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(m) "Investigative or law enforcement officer" means any officer of the state or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this [Act], and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

(n) "Judge of competent jurisdiction" means a judge of any court of general criminal jurisdiction of the state.

(o) "Oral communication" means any verbal communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation. However, such term excludes any electronic communication.

(p) "Pen register" means a device which records or

decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. However, such term excludes any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider of any device used by a provider, or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(q) "Person" means any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

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

(1) scrambled or encrypted;

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

(3) carried on a subcarrier or other signal subsidiary to a radio transmission;

(4) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

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

(s) "Trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

(t) "User" means any person or entity who:

(1) uses an electronic communication service; and

(2) is duly authorized by the provider of such service to engage in such use.

(u) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate or foreign communications or communications affecting intrastate, interstate or foreign commerce, including any electronic storage of such communication. However, such term excludes the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

COMMENT

This section defines several terms frequently used in the [Act] and should eliminate ambiguities and ensure uniform interpretations of the defined terms. Subsections (p) and (s) are of particular importance because they precisely describe what pen registers and trap and trace devices.

Section 5. General Prohibition on Pen Register and Trap and Trace Device Use; Exception.

(a) Except as provided in subsection (b), no person may install or use a pen register or a trap and trace device without first obtaining a court order under Section 7 of this [Act].

(b) The prohibition of section (a) is inapplicable with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service:

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) 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 communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) A person who knowingly violates subsection (a) shall be fined [$5,000.00] for each violation, or imprisoned not more than [one year], or both.

COMMENT

Generally, court orders are prerequisites for installing or using any pen register or trap and trace device per Section 7 of this [Act]. However, there are several exceptions that are outlined in subsection (b). Subsection (b) allows a provider of electronic or wire communication service to use or install the device without first obtaining a court order if the device relates to the operation, maintenance, and testing of the services. A court order is also unnecessary if the device protects the rights or property of the provider, or protects the user from abuse or unlawful use of service.

Paragraph (b)(2) allows providers to record that a communication was initiated or completed. The content of the communication is not to be recorded in order to protect providers and subscribers of the service from fraudulent, unlawful, or abusive use of the service.

Subsection (c) imposes a penalty for knowingly installing or using a prohibited device without a court order.

Section 6. Application for an Order for a Pen Register or Trap and Trace Device.

(a) A state investigative or law enforcement officer authorized by the attorney for the state may make application in writing under oath or equivalent affirmation to a court of competent jurisdiction for an order or an extension of an order under Section 7 of this [Act] authorizing or approving the installation and use of a pen register or a trap and trace device under this [Act].

(b) An application under subsection (a) shall include:

(1) the identity of the attorney for the state or the law enforcement or investigative 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.

COMMENT

This section outlines the procedure and requirements for law enforcement authorities to obtain a pen register or trap and trace. Authorities must submit a written application under oath or equivalent affirmation to the court with jurisdiction.

The application must identify the attorney or law enforcement officer, the agency conducting the investigation, and a certification by the applicant that the sought after information is relevant to the agency's ongoing criminal investigation.

The relative simplicity of the application makes court orders readily available for legitimate purposes while the requirement that the application be made under oath should deter authorities from frivolous investigations that may infringe upon individual rights.

Section 7. Issuance of an Order for a Pen Register or a Trap and Trace Device.

(a) Upon an application made under Section 6 of this [Act], 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 attorney for the state or law enforcement or investigative 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.

(b) An order issued under this section:

(1) 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 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; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installa-

tion of the pen register or trap and trace device under Section 8.

(c) An order issued under this section:

(1) shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed 60 days; and

(2) may be granted only upon an application for an order under Section 6 of this [Act] after a judicial finding required by subsection (a). The period of extension shall not exceed 60 days.

(d) 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;

(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; and

(3) a violation of this subsection may be punished as a contempt of the issuing or denying judge.

COMMENT

This section lists the elements of a court order, time limitations on that order, and the penalty imposed when that order is violated.

The court will grant the order if the court is convinced that the sought after information is relevant to an ongoing criminal investigation.

The order itself shall identify the person who owns or leases the telephone line to the attached device, the person, if known, who is the subject of the criminal investigation, the telephone number, the physical location or geographic limits of the surveillance if known, and the offense the device is being used to expose or prove. Information, facilities, and technical assistance can also be provided by court order if the applicant so requests.

The elements of the court order are specifically documented in order to prevent unnecessary invasions of privacy, mistakes including, "bugging" the wrong line, or exclusion of the intercepted information at trial due to an improper or illegal search.

The surveillance devices can be used for up to but not exceeding 60 days. An extension can be granted for an additional 60 days provided an application that fulfills the requirements of Section 6 is approved by the court. These time limitations protect individual rights of privacy by preventing the authorities from abusing the surveillance privileges, i.e. continuing to monitor a subject after the particular investigation is completed just to keep tabs on the subject.

The court order authorizing the device will be sealed to prevent the subject from being tipped off to the surveillance. Additionally, the service provider and/or any entity involved will be forbidden to disclose the existence of the device to anyone especially the subscriber. If necessary, a separate court order may lift these restrictions.

Lastly, the section details the fact that the issuing or denying judge may charge anyone who violates this subsection with contempt of court.

Section 8. Assistance in Installation and Use of a Pen Register or a Trap and Trace Device.

(a) Upon the request of the attorney for the state or an officer of a law enforcement agency authorized to install and use a pen register under this [Act], 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 with the service that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in Section 7(b)(2) of this [Act].

(b) Upon the request of the attorney for the state or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this [Act], a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the

installation and use is to take place, if such installation and assistance is directed by a court order as provided in Section 7(b)(2) of this [Act]. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to Section 7(b) or Section 9 of the [Act], to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) 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 such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities or assistance in accordance with the terms of a court order under this [Act] or request pursuant to Section 9 of this [Act].

(e) A good faith reliance on a court order under this [Act], a request pursuant to Section 9 of this [Act], a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this [Act].

COMMENT

This section requires providers of communications services, landlords, custodians, or other people in a position to help with a court ordered surveillance, to offer their assistance in installing and using the pen register with the least amount of interference and obtrusiveness.

The same assistance is required in the installation and use of trap and trace devices. The results obtained by this device will be provided to the agency identified in the court order at reasonable intervals during business hours for the duration of the court order.

In return for their assistance, those who cooperated will be reasonably compensated for the reasonable expenses they incurred during their assistance. In addition, service providers, their officers, agents, employees, and other specified persons are immune from liability for certain causes of action. Furthermore, the providers' good faith reliance on court orders, Section 9 requests, legislative authorizations, or statutory authorizations are complete defenses to either civil or criminal actions that do proceed. As a result, providers and others who assist the law enforcement agencies are not punished or disadvantaged. In fact, the agencies become risk-fee clients or customers.

Section 9. Emergency Pen Register and Trap and Trace Device Installation.

(a) Notwithstanding any other provision of this [Act], any investigative or law enforcement officer, specially designated by the attorney for the state may have installed and use a pen register or trap and trace device if:

(1) the officer reasonably determines that:

(A) an emergency situation exists that involves:

(i) immediate danger of death or serious bodily injury to any person; or

(ii) 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, with due diligence, be obtained; and

(B) there are grounds upon which an order could be entered under this [Act] to authorize such installation and use; and

(2) within 48 hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with Section 7 of this [Act].

(b) In the absence of an authorizing order, such use shall immediately terminate upon the earlier of obtainment of the information sought, denial of the application, or the lapse of 48 hours since the installation of the pen register or trap and trace device.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within 48 hours of the installation shall constitute a violation of this [Act] and shall make such person liable to the penalties outlined in Section 5(c) of this [Act].

(d) A provider for a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

COMMENT

This section defines when an emergency situation exists, who has the authority to make and act on that determination, and the procedures, limitations, and potential penalties involved in an emergency authorization without a court order.

Investigative or law enforcement officers, specifically designated by the attorney for the state are the only ones designated in this [Act] to determine whether an emergency situation exists. An emergency situation can exist when there is the possibility of immediate death or serious bodily injury to any person. Another emergency situation can involve the need to install a pen register or trap and trace device before a court order can be obtained with due diligence in order to monitor conspiratorial activities of organized crime. This is an emergency only if there are sufficient grounds for a court order, and one is issued within 48 hours after the installation occurred or begins to occur. If an authorized officer decides there are sufficient grounds for a court order although there is no time to get one, the officer may install the device if again an order is issued within 48 hours of the installations or use occurred or begins to occur.

The amount of time allotted to an emergency authorization is extremely limited to prevent abuses and any invasion of an individual's rights. The emergency authorization expires at the earliest of the following events: when the information sought is obtained, when the application for the court order is denied, or when 48 hours have lapsed since the installation of the device.

A fine, imprisonment, or both according to the penalties imposed by Section 5(c) may await one who knowingly installed a device without applying for a court order within 48 hours of the installation.

As in Section 8(c), providers of assistance to law enforcement agencies will be reasonably compensated for the reasonable expenses of their assistance.

Section 10. Reports Concerning Pen Registers and Trap and Trace Devices.

The attorney general shall annually report to the legislature on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the state.

Section 11. Unlawful Interception and Disclosure of Wire, Oral, or Electronic Communications.

(a) Except as provided in subsection (c), it is unlawful for a person to intentionally:

(1) intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(2) use, endeavor to use, or procure any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(A) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(B) such device transmits communications by radio, or interferes with transmission of such communication; or

(C) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in intrastate, interstate or foreign commerce; or

(D) such use or endeavor to use:

(i) takes place on the premises of any business or other commercial establishment the operations of which affect intrastate, interstate or foreign commerce; or

(ii) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect intrastate, interstate or foreign commerce;

(3) disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(4) use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

(b) A person who violates subsection (a) shall be punished as provided in subsection (e) or shall be subject to suit as provided in subsection (f).

(c) It shall be lawful under this [Act] for:

(1) an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of that person's employment while engaged in any activity which is a necessary incident to the rendition of that person's service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks;

(2) (A) providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with:

(i) a court order directing such assistance signed by the authorizing judge; or

(ii) a certification in writing by the attorney for the state that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. The certification shall set forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

(B) No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this [Act], except as may otherwise be required by legal process and then only after prior notification to the attorney for the state as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in Section 19 and for contempt of court as provided in Section 17.

(C) No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this [Act].

(3) a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception;

(4) a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state;

(5) a person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(6) a person to intercept any radio communication which is transmitted:

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

(B) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(C) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio service; or

(D) by any marine or aeronautical communications system;

(7) a person to engage in any conduct which:

(A) is prohibited by Section 633 of the Communications Act of 1934; or

(B) is excepted from the application of Section 705(a) of the Communications Act of 1934 by Section 705(b) of that Act;

(8) a person to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference;

(9) other users of the same frequency to intercept any radio communication made through a system that utilized frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted;

(10) a person to use a pen register or a trap and trace device as those terms are defined in this [Act]; or

(11) 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.

(d) (1) Except as provided in paragraph (2) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity, or an agent thereof, while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(2) A person or entity providing electronic communication service to the public may divulge the contents of any such communication:

(A) as otherwise authorized in Section 11(c) or 15 of this [Act];

(B) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(C) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(D) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(e) (1) Except as provided in paragraph (2) of this subsection or in subsection (f), whoever violates subsection (a) of this section shall be fined under this [Act], or imprisoned not more than five years, or both.

(2) If the offense is the first offense under paragraph (1) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (1) is a radio communication that is not scrambled or encrypted, then:

(A) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (f), the offender shall be fined under this [Act], or imprisoned not more than [one year], or both; and

(B) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication or a paging service communication, the offender shall be fined not more than [$500].

(3) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted:

(A) to a broadcasting station for purposes of retransmission to the general public; or

(B) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(f) (1) (A) If the communication is:

(i) a private satellite video communication

that is not scrambled or encrypted and the conduct in violation of this [Act] is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(ii) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this [Act] is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the state in a court of competent jurisdiction.

(B) In an action under this subsection:

(i) if the violation of this [Act] is a first offense for the person under paragraph (1) of subsection (e) and such person has not been found liable in a civil action under Section 19 of this [Act], the state shall be entitled to appropriate injunctive relief; and

(ii) if the violation of this [Act] is a second or subsequent offense under paragraph (1) of subsection (d) or such person has been found liable in any prior civil action under Section 19, the person shall be subject to a mandatory [$500] civil fine.

(2) The court may use any means within its authority to enforce an injunction issued under paragraph (f)(1)(B)(i), and shall impose a civil fine of not less than [$500] for each violation of such an injunction.

COMMENT

Generally, it is unlawful for any person to intercept or attempt to intercept any wire, oral, or electronic communication. This section describes when the uses of any electronic, mechanical, or other devices are prohibited. Devices that in some way use wirelike connections or radio communications are prohibited as well as those that interfere with radio communication. A person is also prohibited from using such a device passed through the mail, interstate, intrastate, or foreign commerce.

Disclosing and/or using the contents of any wire, oral, or electronic communication violates the [Act] if the person disclosing or using the contents knew or should have known that the contents were obtained through interception.

The blanket punishment stated in subsection (d) imposes a fine under the [Act], imprisonment, or both. The punishments differ for violations of subsection (a) depending on whether the violation was a first offense, what kind of motive was behind the violation, and the manner of the interception.

If a first time offender had no tortious, illegal, or improper motive including private or commercial gain, and the communication is an unscrambled or encrypted radio communication then the exact type of radio communication used must be determined. If the communication is not a radio portion of a cellular phone, a public land mobile radio service, or a paging service, the offender will be fined or imprisoned for not more than one year, or both. If the communication is one of the above then the offender will be fined not more than [$500].

There is no violation if a person intercepts a satellite transmission that is not encrypted or scrambled, and that is transmitted to a broadcasting station with the intention of being transmitted to the public. However, if a person, with the purposes of commercial advantage or private financial gain, intercepts an audio subcarrier intended for redistribution to facilities open to the public, that person has violated the [Act]. However, there would not be a violation without the improper motive. Data transmissions and telephone calls are also prohibited from being intercepted, and those responsible are subject to fines and/or imprisonment.

Subsection (a) also cites subsection (f) to determine where violators are subject to suit, what monetary or injunctive relief is available, and who enforces the relief that is granted. If a person pirates or intercepts satellite video communications for their own viewing pleasure with any other aforementioned improper motives or they intercept a radio communication on a special Federal Communications Commission frequency without an improper motive, they are to be sued by the state in a court of competent jurisdiction.

If a first time offender according to subsection (f) avoids liability in a civil action, the state is entitled to injunctive relief. The court can enforce this injunction, and can impose a mandatory fine for each violation of the injunction.

Subsection (a)'s restrictions on the interception, use, and disclosure of wire, oral, and electronic communications are extensive, but they do not include these people whose jobs necessarily or unavoidably violate these restrictions. Under subsection (c), switchboard operators, officers, employees, or agents of providers of wire or electronic services will not be charged with violating the statute if the violations they commit are incident to or protect the service to the public. There is one caveat, however. Service providers cannot observe or randomly monitor communications except for mechanical or service quality control checks.

Similar to the sections pertaining to pen registers and trap and trace devices, those who assist persons authorized by law to intercept communications or conduct surveillance do not violate the statute as long as they have a valid court order. A letter from the attorney for the state certifying that no warrant or court order is required by law, all statutory requirements have been met, and specifying the assistance and time the authorities need, will suffice for authorization.

Again, those who assist are prohibited from disclosing the fact that they are assisting the law enforcement agency and the contents of the communications they intercepted. They can only disclose with the permission of court order and appropriate notice to the attorney for the state.

If those who assist comply with these rules, they will be immune from any cause of action against them resulting from their involvement with the law enforcement agency. If they disclose, they will be liable for civil damages per Section 19 and contempt of court per Section 17.

The [Act] also allows parties to the communication or those who have the permission of one of the parties to the communication to intercept a communication. The only limitation on those interceptions is that the intent behind the interception not be to violate the Constitution and laws of the United States or any individual state.

Subsection (c) creates obvious exceptions that involve individual and public safety as well as frequencies voluntarily made available to the public. Generally, if a signal, electronic, or radio communication is readily accessible to the general public, it is not unlawful for the public to access that communication or transmission. The accessible transmissions include commercial, CB, and ham radios, and the accessible communications include marine or aeronautical communications. Subsection (c)(6) allows the access, interception, or use of distress signals for people, vehicles, or vessels in order to provide necessary aid or assistance. The same goes for radio communications emitted by governmental, law enforcement, or private land mobile safety systems to inform the public of existing or potential hazards.

Subsection (c)(8) allows interception of wire or electronic communications that cause harmful interference to radio stations or consumer electronic equipment in order to identify the cause and source of the interference. Under subsection (c)(9), users of the same frequency who intercept an unscrambled radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or use of such system, do not violate the [Act].

To maintain continuity and consistency among the various sections of the [Act], subsection (c)(10) and (11) restate that the use of pen registers and trap and trace devices is legal and that service providers can record that fact that a wire or electronic communication was initiated or completed to protect themselves, their colleagues, and their customers from fraudulent, unlawful, or abusive service.

Subsection (d) addresses what contents of communications providers of electronic communication services can and cannot intentionally divulge. Generally, they cannot divulge anything except to the intended recipient of the communication or their agent. The providers are permitted to divulge contents if they are authorized to do so under Sections subsection (c)(1) and Section 15 of the [Act], or if they are given permission by the originator or intended recipient. Providers are also permitted to divulge contents to those employed or authorized to forward the communication to its recipient i.e., secretaries and answering services. Lastly, providers are only permitted to divulge to a law enforcement agency the contents of any communication that was inadvertently obtained which appears to be related to a crime.

Section 12. Unlawful Manufacture, Distribution, Possession, and Advertising of Wire, Oral, or Electronic Communication Intercepting Devices.

(a) Except as provided in subsection (c), it is unlawful for any person to intentionally:

(1) send through the mail, or send or carry in intrastate, interstate or foreign commerce, any electronic, mechanical, or other device, knowing or

having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communication;

(2) manufacture, assemble, possess, or sell any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in intrastate, interstate or foreign commerce; or

(3) place in any newspaper, magazine, handbill, or other publication any advertisement of:

(A) any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of surreptitious interception of wire, oral, or electronic communications; or

(B) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in intrastate, interstate or foreign commerce.

(b) A person who violates subsection (a) shall be fined not more than [$10,000], or imprisoned not more than [five years], or both.

(c) Notwithstanding subsection (a), it shall be lawful for a person to send through the mail, send or carry in intrastate, interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, if the person is:

(1) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service; or

(2) an officer, agent, or employee of, or a person under contract with, the United States, a state, or a political subdivision thereof, in the normal course of the activities of the United States, a state, or a political subdivision thereof.

COMMENT

Section 12 attempts to curb the availability of surveillance equipment to the general public to control its use in criminal activities. It applies a three pronged approach to stop the intentional manufacture, assembly, possession, or sale of surveillance equipment by cutting off the transportation and advertising of the products.

First, the section cuts off the option of using independent shipping and delivery companies by prohibiting those who send or carry products they know or should know are primarily used for surreptitious interception from using the mail or carrying them in interstate, intrastate, or foreign commerce. The "should know" clause is used to thwart the companies' intentional ignorance of the contents of the companies' deliveries or cargo.

Second, the section directly attacks the manufacturers, assemblers, possessors, and sellers of devices they know or should know will be primarily used for surreptitious interception. It prohibits them from shipping, carrying, or mailing their products in interstate, intrastate, or foreign commerce.

Third, the section prohibits people from intentionally advertising in newspapers, magazines, handbills, or other publications. If a person knows or has reason to know that the product they are advertising is primarily used for surreptitious interception of wire, oral, or electronic communications, they are prohibited from placing the ad. The same goes for advertising that promotes the use of the equipment for surreptitious interception if the advertiser knows or should know the ad will be sent or carried in the mail or interstate, intrastate, or foreign commerce.

Section 12 also creates exceptions that allow providers of wire or electronic services, their employees, officers, agents, and those who are under contract with the United States, a state, or their many divisions to mail, carry, manufacture, assemble, possess, or sell any device they know or should know to be primarily useful for purposes of surreptitious interception of wire, oral, or electronic communications.

Section 13. Confiscation of Wire, Oral, or Electronic Communication Interception Devices.

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of this [Act] is hereby declared a nuisance and may be seized and forfeited to the state.

Section 14. Prohibition of Use as Evidence of Intercepted Wire or Oral Communications.

No part of the contents of any wire or oral communication intercepted in violation of this [Act], and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of this state, or political subdivision thereof.

COMMENT

This section makes any improperly intercepted communication or the fruits thereof inadmissible in any proceeding. This exclusionary rule eliminates the possibility of reaping benefits from an illegal interception.

Section 15. Authorization for Interception of Wire, Oral, or Electronic Communications.

(a) The attorney for the state may authorize an application to a judge of competent jurisdiction for, and such judge may grant in conformity with Section 17 of this [Act] an order authorizing or approving the interception of wire or oral communications by an investigative or law enforcement officer, or an agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of:

(1) any offense punishable by death or by imprisonment for more than one year;

(2) any offense which involves murder, kidnapping, robbery, or extortion;

(3) any of the following offenses: [bribery of public officials and witnesses], [relating to bribery of bank officials], [bribery in sporting contests], [unlawful use of explosives], [relating to concealment of assets], [transmission of wagering information], [relating to escape], [relating to loans and credit applications generally; renewals and discounts], [influencing or injuring an officer, juror, or witness generally], [obstruction of criminal investigations], [obstruction of state or local law enforcement], [interference with commerce by threats or violence], [intrastate, interstate and foreign travel or transportation in aid of racketeering enterprises], [relating to violent crimes in aid of racketeering activity], [prohibition of business enterprises of gambling], [violation of the Model Money Laundering Act or similar state law], [theft from intrastate, interstate shipment), [fraud by wire, radio, or television], [relating to bank fraud], [sexual exploitation of children], [intrastate and interstate transportation of stolen property], [relating to trafficking in certain motor vehicle or motor vehicle parts], [relating to hostage taking], [relating to penalty for failure to appear], [violation of Model Ongoing Criminal Conduct Act or similar state law];

(4) any felony violation of the [state controlled substances act, [Model State Chemical Control Act] or similar state law, or other applicable state law involving controlled substances or other dangerous drugs];

(5) any felony violation of Sections 11 and 12;

(6) any felony violation [relating to obscenity];

(7) any felony violation [relating to firearms];

(8) any conspiracy to commit any offense described in this subsection;

(9) the location of any fugitive from justice from an offense described in this subsection;

(b) The attorney for the state may authorize an application to a judge of competent jurisdiction for, and such judge may grant, in conformity with Section 17 of this [Act], an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made.

COMMENTS

The attorney for the state may authorize an application for a court order permitting an interception. The section lists the offenses for which an application may be sought in the course of an investigation.

Section 16. Authorization for Disclosure and Use of Intercepted Wire, Oral, or Electronic Communications.

(a) Any investigative or law enforcement officer who, by any means authorized by this [Act], has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may:

(1) disclose such 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; or

(2) use such contents to the extent such use is appropriate to the proper performance of the officer's official duties.

(b) Any person who has received, by any means authorized by this [Act], any information concerning a wire, oral, or electronic communication, or evidence derived therefrom, intercepted in accordance with the provisions of this [Act] may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of this state or political subdivision thereof.

(c) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this [Act] shall lose its privileged character.

(d) An investigative or law enforcement officer engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, who intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, may disclose or use the contents thereof, and evidence derived therefrom, as provided in subsection (a) of this section. Such contents and any evidence derived therefrom may be used under subsection (b) of this section if a judge of competent jurisdiction so authorizes after finding on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this [Act]. Such application shall be made as soon as practicable.

COMMENTS

Section 16 addresses how the contents of a properly intercepted communication may be used once they are obtained. Investigative or law enforcement officers can use the information in the course of their official duties if the information is appropriate to those duties. An officer may also disclose the contents to a fellow officer if the contents will help either officer fulfill the officer's official duties.

Any person can disclose the contents of a properly intercepted communication while testifying under oath or affirmation in any state proceeding. However, if the obtained information is privileged in some way, the privilege remains, and the information is treated accordingly.

Subsection (d) addresses the situation when the contents of a properly intercepted communication relate to an offense other than the offense specified in the court order of authorization. It may be used by officers or disclosed to other officers to perform official duties of law enforcement under subsection (a). The contents may be discussed in testimony under oath if a subsequent application for authorization is submitted as soon as practicable and is approved by a judge under this [Act]. This section outlines how and under what circumstances lawfully intercepted communications may be disclosed.

Section 17. Procedure for Interception of Wire, Oral, or Electronic Communications.

(a) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this [Act] shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state:

(1) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(2) the applicant's authority to make such application;

(3) fully and completely 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) except as provided in subsection (o) of this section, 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) fully and completely 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) 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;

(5) fully and completely 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; and

(6) where the application is for the extension of an order, the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

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

(c) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic 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 offense enumerated in Section 15 of this [Act];

(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; and

(4) except as provided in subsection (o), 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 such offense, or are leased to, listed in the name of, or commonly used by such person.

(d) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this [Act] 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; 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.

(e) An order authorizing the interception of a wire, oral, or electronic communication under this [Act] shall, upon request of the applicant, direct that a provider of wire or electronic communication service, 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 service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or

technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

(f) An order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for the shorter of 30 days or the period necessary to achieve the objective of the authorization. Such 30 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 only upon application for an extension made in accordance with subsection (a) of this section and the court making the findings required by subsection (c) of this section. The period of extension shall be the shorter of 30 days or the time the authorizing judge deems necessary to achieve the purposes for which it was granted. 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 [Act], and must terminate upon the earlier of 30 days or the attainment of the authorized objective. 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.

(g) An interception under this [Act] may be conducted in whole or in part by state, county or municipal personnel, or by an individual operating under a contract with the state, county or municipality acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(h) Whenever an order authorizing interception is entered pursuant to this [Act], 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.

(i) Notwithstanding any other provision of this [Act], any investigative or law enforcement officer, specially designated by the attorney for the state, may intercept a wire, oral or electronic communication prior to issuance of an order approving the interception if:

(1) the 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 requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained; and

(B) there are grounds upon which an order could be entered under this [Act] to authorize such interception; and

(2) an application for an order approving the interception is made in accordance with this section within 48 hours after the interception has occurred, or begins to occur.

(j) In the absence of an order approving an interception described in subsection (i), such interception shall immediately terminate upon the earlier of obtainment of the communication sought or denial of the application.

(k) In the event an application for approval of an interception described in subsection (i) is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this [Act], and an inventory shall be served as provided for in subsection (p)(4) of this section on the person named in the application.

(l) (1) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this [Act] shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection 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, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under the judge's directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use

or disclosure pursuant to the provisions of Section 16(a) of this [Act] for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, under Section 16(b).

(2) Applications made and orders granted under this [Act] shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(3) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(4) Within a reasonable time, not to exceed 90 days, after the filing of an application for an order of approval under subsection (k) 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 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, approved or disapproved interception, or the denial of the application; and

(C) 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 make available to such person or such person's 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 inventory required by this subsection may be postponed.

(m) The contents of any wire, oral, or electronic communication intercepted pursuant to this [Act], or evidence derived therefrom, shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a court of this state 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. This ten day period may be waived by the judge if the judge finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(n) (1) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of this state, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this [Act], or evidence derived therefrom, on the grounds that:

(A) the communication was unlawfully intercepted;

(B) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(C) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this [Act]. The judge, upon the filing of such motion by the aggrieved person, may make available to the aggrieved person or such person's counsel for inspection such portions of the intercepted communication, or evidence derived therefrom, as the judge determines to be in the interests of justice.

(2) In addition to any other right to appeal, the state shall have the right to appeal from an order granting a motion to suppress made under paragraph (1) of this subsection, or the denial of an application for an order of approval, if the attorney for the state certifies to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the

date the order was entered and shall be diligently prosecuted.

(3) The remedies and sanctions described in this [Act] with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this [Act] involving such communications.

(o) The requirements of subsections (a)(3)(B) and (c)(4) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted are inapplicable if:

(1) in the case of an application with respect to the interception of an oral communication:

(A) the application is by an investigative or law enforcement officer and is approved by the attorney for the state;

(B) the application contains a full complete statement as to why such specification is not practical and identifies the person committing the offenses and whose communications are to be intercepted; and

(C) the judge finds that such specification is not practical; and

(2) in the case of an application with respect to a wire or electronic communication:

(A) the application is by an investigative or law enforcement officer and is approved by the attorney for the state;

(B) 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

(C) the judge finds that such purpose has been adequately shown.

(p) An interception of a communication under an order to which the requirements of subsections (a)(3)(B) and (c)(4) of this section do not apply by reason of subsection (o) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (o)(2) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the state, shall decide such a motion expeditiously.

COMMENTS

Section 17 is a broad section of the [Act] that covers nine topics. Section 17 illustrates the elements of a valid application for the authorization of an interception; lists what is necessary for a judge to approve that application; describes the elements of the court order itself and what that order specifically authorizes; lays out the procedures for emergency situations, and procedures for preserving the records of applications, authorizations, and orders; and includes information regarding notice to opposing parties and motions to suppress. Rounding out Section 17's topics are penalties and sanctions for violations of the section and exceptions to certain requirements for authorization.

The first topic Section 17 covers is the elements of the application requesting authorization to intercept communications. A judge of competent jurisdiction must receive a written application made under oath or affirmation that states the applicant's authority to submit such an application. The application must also identify both the investigative or law enforcement officer making the application and the officer authorizing the application.

The applicant should then describe the case itself by providing all of the facts of the case including the details of the suspected offense, the description and location of the targeted facility, the type of communications to be intercepted, and the identity, if known, of the targeted person. The applicant should also include information about other investigative techniques that were either used and failed or not attempted because they seemed doomed from the start. In addition, other applications, known to this perspective applicant, that were submitted to gain authorization to intercept communications of any of the same people as in the current application or at any of the same places must be included.

The application should next describe and discuss the time frame in which the authorization is necessary. If the applicant needs the authorization to continue beyond the time when the sought communication is obtained, the applicant must establish probable cause to believe that those sought after communications will continue. If an extension is requested, the progress or lack of progress of the current interceptions must be included. In addition to all of the above elements or

requirements, a judge may require applicants to furnish testimony or evidence beyond what was originally included.

Judges may approve the application and grant the authorizing order on the basis of the application if four requirements are fulfilled. First, there must be sufficient probable cause that the particular offense is, was, or will be committed. Second, there must be sufficient probable cause that particular communications sought will concern that offense. Third, the judge must determine that normal investigative techniques have been or will likely be unsuccessful or too dangerous. Finally, there must be a determination that the targeted facility is, in fact, leased to, listed in the name of, owned by, or commonly used by that targeted person.

The authorizing order itself is very specific in order to prevent misunderstandings as to what exactly has been authorized, constitutional violations like improper searches, and any problems regarding the admissibility of the recovered evidence. The order lists exactly whose communication will intercepted, where and what kind of place the targeted facility is, and the type of communication to be intercepted. To prevent the order from becoming a blanket order for any agency or person to claim authorization for separate interceptions, the court order also identifies the agency authorized to intercept the communication and the person authorizing the application. Further, the order contains the exact time period allowed for the authorized investigation and whether or not it will be continued beyond the moment when the sought after communication is obtained.

Additionally, the order will direct providers of communications service and those others in a position to give assistance like landlords and custodians to aid the authorized agency in any manner including providing information, equipment, facilities, etc. The agency, in turn, will conduct its investigation with as little interference as possible as well as providing the assistants with reasonable compensation for the reasonable expenses they incurred while aiding the investigation.

The order may only authorize interceptions for the amount of time necessary to obtain the sought information, and that time cannot exceed 30 days. That time begins either on the day the interception begins or ten days after the order is entered, whichever is earlier. A new application must filed to get extensions. The new application should meet all of the requirements of the initial application for the interception including an explanation of the need for the extension. Each extension will be for the amount of time the judge decides is appropriate, and it will be for no longer than 30 days. The time restrictions may be reasonably extended if the targeted communication is in a foreign language or code to allow for the interpretation or translation of intercepted material, and to allow personnel to separate out extraneous communications.

Section 17 also lists those people, agencies, or entities who are able to conduct these types of investigations including the states, countries, or municipalities and those under contract with them. The order may direct them to conduct the interceptions as quickly and efficiently as possible, and to provide the authorizing judge with progress reports.

Emergency situations are the next topic addressed in Section 17. These situations occur when an interception must be conducted immediately, thus without a court order. The circumstances that constitute an emergency situation and the people involved in it are similar to those enumerated in the pen register and trap and trace sections of this [Act]. A law enforcement officer who is either specifically designated by the attorney for the state can make the determination of whether there is an emergency. Only these people are authorized in order to prevent abuse of the emergency provisions. Thus, any officer cannot bypass the court order requirement just because they believe a situation is an emergency.

An emergency can exist in three types of situations. If there is immediate danger of death or serious physical injury to any person, or a conspiracy that threatens national security is involved then an emergency exists. The third type of emergency involves conspiratorial activities characteristic of organized crime that require interception before an order could be authorized with due diligence. In this situation, the agency who conducted the interception must have grounds for the interception in compliance with the [Act]. They must file a complete application within 48 hours after the interception occurred or begins to occur, and the interception must end when the sought after information is obtained or when the order is denied, whichever is earlier.

If the order is indeed denied, then the contents of the communication shall be treated as the product of tainted search or interception. The judge who denied or terminated the order or extension will also provide an inventory to whomever the judge believes to be appropriate. This inventory will be given within 90 days of the filing of the application as provided for in subsection (p)(4). The inventory will include the facts that the application

was filed, an order was entered, the dates they were filed and entered, the disposition of the application, and that the communication was or was not intercepted. The inventory may be postponed if good cause is shown. The parties may also request the judge to grant their motion to inspect the materials.

Section 17 next provides regulations for the storage and use of the recordings of intercepted communications, applications, authorizations, and orders. These regulations are intended to not only protect the privacy of individuals and their communications but also to protect the privacy of law enforcement operations in order to maintain their efficiency. The actual recordings should be on tape, wire, or something comparable, and should be resistant to outside editing to avoid tampering.

After an authorized interception is completed, it is to be turned over to the authorizing judge who will seal it. The communication will be kept for at least ten years unless a judge orders its destruction prior to then. The agency who conducted the interception may use duplicates of the original communication or share them with colleagues if the communication will aid them in their official duties as stated in Sections 16(a). If the communication is to be used as evidence or in a testimony, Section 16(c) requires that communication to be sealed. If there is no seal, it still can be used if the seal's absence is satisfactorily explained.

Applications, authorizations, and orders must also be sealed and kept for ten years unless a judge orders their destruction earlier. The judge will determine where those documents are to be kept. The judge will also determine if they are ever to be disclosed on the basis of good cause. Further, the judge has the power to enforce the preservation of the communications and/or records with a contempt of court charge.

If the contents of an intercepted communication are to be received into evidence or disclosed at any state court proceeding, the application and order authorizing the interception are sent to the opposing party to serve as proper notice. A copy of each must be furnished to the opposing party at least ten days before the proceeding. As in other rules of procedure, the notice may be waived if a judge determines it would be impossible to serve notice at least ten days before trial, and that the party lacking notice would not be prejudiced.

Section 17 further documents the options of each party to the suit. They could oppose the introduction or use of the communication or oppose the order approving the authorization. Motions to suppress the contents of an intercepted wire or oral communication or any evidence derived from them can be entertained in or before <u>ANY</u> state court, department, officer, agency, regulatory body, etc. Claims that the communication was illegally intercepted, that the order authorizing the interception was insufficient on its face, or that the interception violated or went beyond the authorizing order are sufficient grounds for such a motion to suppress. The motion must be filed before the proceeding in which the communications are to be used. If there was no opportunity to file the motion, or if the party was unaware of the grounds for the motion then a late motion may be considered. The judge may also allow the aggrieved party to inspect portions of the communications or evidence according to the judge's discretion.

If the motion to suppress is granted or an application is denied, the state may appeal if the state proves that the appeal is not intended for purposes of delay. That appeal must be filed within 30 days of the day that contested order was entered, and it should be diligently prosecuted.

Section 17 also ensures that the remedies and sanctions provided within this [Act] are the only ones for nonconstitutional violations of Section 17 involving the communications described in it.

Section 17(k) provides exceptions to the requirement that the targeted facility must be specifically described. These exceptions allow authorizations even though some application requirements are impossible to comply with. In the case of an oral communication, first the investigative or law enforcement officer's application is approved by the attorney for the state. Second, the application must completely explain why the specification is impractical, identify the subjects of the offense, and identify whose communications are to be intercepted. Third, the judge must agree that it is impractical to provide the specifications. In the case of a wire or electronic communication, the requirements mirror those in an oral communication except the application must show that the subject is purposely thwarting interception by changing facilities and the judge agrees that the purpose was shown.

If the judge does not allow the application to be proved without the specifications, the interception cannot begin until the target facility is ascertained by the person implementing the interception order. In addition, a service provider may move to quash an order because its assistance with respect to the interception cannot be per-

formed in a timely or reasonable fashion. The judge will then decide the motion quickly to avoid delay, waste, or the loss of the suspect.

This section also provides a procedure for emergency intercepts. This section requires that, if possible, all intercepted information should be recorded for future judicial review; mandates the sealing and storage of all applications and orders and sets a time limit for their destruction; and provides a penalty of contempt of court for any violations of this section. Section 17 also provides for notification of parties against whom intercept orders were granted and the procedures for those parties to challenge said orders and their results. This section establishes an appeal procedure for state officials in the event of adverse rulings and allows service providers to challenge an intercept order on the grounds that the intercept cannot be performed in a timely or reasonable fashion.

Section 18. Reports Concerning Intercepted Wire, Oral, or Electronic Communications.

(a) Within 30 days after the expiration of an order, or each extension thereof, entered under Section 17, or the denial of an order approving an interception, the issuing or denying judge shall report to the [appropriate court official]:

(1) the fact that an order or extension was applied for;

(2) the kind of order or extension applied for, including whether or not the order was an order with respect to which the requirements of Sections 17(a)(3)(B) and 17(c)(4) of this [Act] did not apply by reason of Section 17(k) of this [Act];

(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 applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(7) the nature of the facilities from which or the place where communications were to be intercepted.

(b) In [appropriate month] of each year the attorney general shall report to the [appropriate court official]:

(1) the information required by paragraphs (1) through (7) of subsection (a) of this section with respect to each application for an order or extension made during the preceding calendar year;

(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) of this subsection with respect to orders or extensions obtained in a preceding year.

(c) In [appropriate month] of each year the [appropriate court official] shall transmit to the legislature a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this [Act] and the number of orders and extensions granted or denied pursuant to this [Act] during the preceding year. Such report shall include a summary and analysis of the data required to be filed with the [appropriate court official] by subsections (a) and (b) of this section. The [appropriate court official] is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (a) and (b) of this section.

COMMENTS

Section 18 sets up a reporting system that runs from the courts and the attorney general to the [appropriate court official], and from the [appropriate court official] to the legislature in order to create an accurate record of intercepted wire, oral, or electronic communications. In case of appeals, new suits, etc., the issuing or denying judge must file a report to the [appropriate court official] within 30 days of the completion of the order or its extensions. The report should include the fact that an order was applied for, the type of such order including any exceptions that were requested like the waiver of specifying the target facilities, and whether the order was granted, modified, or denied. The report must also state the time allowed and any extensions of it, the offense specified in the order or exceptions, the identities of the investigative or law enforcement officer and the person who authorized their application, and the nature of the targeted facilities.

The attorney general must file a report chronicling the interceptions of the previous year and documenting the results therefrom. In general, the report documents the success or failure of using interception as a surveillance technique. The report should include all that the issuing or denying judge reported to the [appropriate court official] plus a general description of the interceptions made under the judge's order. The descriptions will document the approximate nature and frequency of both incriminating communications and other extraneous communications intercepted. The approximate number of persons whose communications were intercepted and an approximate description of the money, time, and resources expended should be included.

The attorney general's report should also provide other result-related statistics like the number of arrests, the number of trials, the total number of motions to suppress, the number of those motions that were granted or denied, and the number of convictions resulting from interceptions. In addition to those numbers, the attorney general must list the offenses the suspects were arrested and/or convicted for, as well as a general assessment of the importance of interceptions.

It is important to note that the [appropriate court official] has the authority to issue binding regulations as to the content and form the judges and attorney general file. On the next level of the hierarchy, the [appropriate court official] must submit a report to the legislature. The report must include numbers of applications for orders authorizing interceptions, and the numbers that were granted or denied. These statistics should pertain to the preceding year. The report should also provide a summary and analysis of the listed data.

Section 19. Authorized Recovery of Civil Damages.

(a) Except as provided in Section 11(c)(2), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this [Act] may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) In an action under this section, appropriate relief includes:

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) (1) In an action under this section, if the conduct in violation of this [Act] is the private viewing of a private satellite video communication that is scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted, and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engages in that conduct has not previously been enjoined under Section 11(f) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than [$50] and not more than [$500].

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under Section 11(f) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than [$100] and not more than [$1000].

(2) In any other action under this section, the court may assess as damages whichever is the greater of:

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) [$100] a day for each day of violation; or

(C) [$10,000]; or

(D) statutory damages.

(d) A complete defense against any civil or criminal action brought under this [Act] is a good faith reliance on:

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under Section 17(i) of this [Act]; or

(3) a good faith determination that Section 11(d) of this [Act] permitted the conduct complained of.

(e) A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

COMMENTS

Section 19 authorizes civil damages to those who were injured because their wire, oral, or electronic communications were intercepted, disclosed, or intentionally used in violation of this statute. Those damages will recovered from the person or entity who violated the statute.

The injured party may receive appropriate preliminary relief, other equitable relief, or declaratory relief, as well as reasonably incurred attorney's fees and litigation costs. Punitive damages may also be available. The damages themselves are computed according to the type of communication intercepted or used and the violator's motive.

The private viewing of a scrambled or encrypted private satellite video communication and the interception and/or use of an unscrambled, unencrypted radio communication that is transmitted on frequencies under subpart D of part 74 of the Federal Communications Commission rules are treated differently in regard to damages than all other types of communications as long as there is no improper motive behind the violations pertaining to them. An improper motive is one for tortious or illegal purposes, or for indirect or direct financial gain.

Generally, the court can assess the greater of the sum of the plaintiff's actual damages plus any profits the violator earned as a result of the violation, or statutory damages. Offenders who have not been enjoined under Section 11(f) as a first time offender not found liable in a prior civil action under Section 19, the offender shall be penalized the greater of the amount of actual damages the plaintiff suffered or statutory damages.

If the offender had been previously enjoined under Section 11(f) or was found liable in a civil action, the court shall impose a fine in an amount equal to the greater of the sum of actual damages the plaintiff suffered or statutory damages.

Section 19(d) outlines complete defenses afforded to an offender who relied in good faith that the offender was complying with the statute. If a suspected offender had a good faith reliance on a court warrant or order, a grand jury subpoena, legislative authorization or statutory authorization, the offender has a complete defense against any civil or criminal action brought under the [Act]. The same goes for good faith reliance on a request of an investigative or law enforcement officer under Section 17(i) in an emergency situation or a good faith determination that Section 11(c) permitted them to intentionally divulge information.

Section 19 also states the statute of limitations on civil actions under this [Act]. An action must be commenced within two years of the date the plaintiff had reasonable opportunity to discover the violation.

Section 20. Injunction Against Illegal Interception.

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this [Act], the attorney for the state may initiate a civil action in [appropriate court] of this state to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the state or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the state Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the state Rules of Criminal Procedure.

COMMENTS

The attorney for the state can file for injunctive relief in state court against anyone who appears about to engage or be engaging in a felony violation of this [Act]. The court may enter a restraining order, a prohibition, or any action before the final determination of the case to prevent continuing or substantial injury to the state or any person.

Section 21. Severability.

If any provisions of this [Act] or application thereof to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of the [Act] which can be given effect without the invalid provisions or application, and to this end the provisions of this [Act] are severable.

Section 22. Effective Date.

This [Act] shall be effective on [reference to normal state method of determination of the effective date][reference to specific date].

Appendix E

National District Attorneys Association Case Summaries: Wiretap and Electronic Surveillance

ORGANIZED CRIME

Multi-Million Dollar Bookmaking Operation

A recent prosecution involved an organized crime individual named Ronald Sacco and his associates. In October, 1988, search warrants were executed in Las Vegas and Los Angeles at approximately a dozen different locations resulting in the break up of a multi-million dollar bookmaking operation.

The probable cause for the search warrants was gained partially through surveillance but mostly through pen registers and phone taps which showed a pattern of communications between "suspect", locations and "known" locations (betting information services, residences of known or convicted book makers, etc.). Telephones are obviously the life support system of this type of crime and we have, of course, found the same to be true of the narcotics trade.

Jewelry Theft and Triple Homicide

Our most consequential wiretap case involved a triple homicide occurring December 11, 1985 in Clark County (Las Vegas), Nevada. These homicides occurred inside the Tipton residence and were motivated by the theft of a large amount of jewelry. Telephone communications between the principals and those involved in the distribution of the jewelry resulted in the drafting and execution of search warrants, the recovery of some of the jewelry and successful prosecution of the principals. Steven Michael Homick is presently on death row and is undergoing prosecution in the State of California for a double homicide alleged to be a contract killing. That prosecution was made possible as a direct result of the electronic intercepts.

NOTE: Although we utilize electronic surveillance sparingly, it has proven to be a remarkably successful investigative tool. Evidence obtained from electronic surveillance in narcotics cases, illegal gambling, murder, pandering and attempted murder / solicitation for murder has been critical to several major prosecutions.

Honorable Rex Bell
District Attorney
Clark County, Nevada

Distict Attorney Investigation Infiltrates Computer Bookmaking Operation

The investigation, begun by the Westchester County District Attorney's Office in February of 1990, and which later became a joint investigation with the United States Customs Service in New York and Dallas, Texas, made extensive use of wiretaps and video surveillance, in both Westchester and Dutchess Counties, where the Dutchess County Narcotics Task Force provided invaluable assistance. The investigation also involved, for the first time in New York State, the court ordered electronic accessing of computer information where records of betting activity were stored.

For over a year before the investigation began, James Monteleone and the principal of a Fort Worth currency exchange were collaborating on the development of a computer system specifically created for bookmakers. The system was designed to keep track of scheduled sporting events, the "lines" (or odds) on each event, the names of bettors and other subordinate bookmakers (runners), the amounts each wagered on each event and the commissions earned by members of the operation, and of course, the amount of money won or lost by each bettor on each event and the status of his/her account. The computer system was to be marketed to bookmakers throughout the country and had a unique feature for their benefit. All the data contained in the computer was to be "down loaded" automatically to a main computer in Mexico where a duplicate set of the bookmakers' records would be stored indefinitely. Should the police raid the bookmaker's office, (the theory went) he need only type a combination of letters into the computer which would erase the entire program, leaving prosecutors with no gambling records to use as evidence. After the police would leave the office empty handed, the bookie could, for a fee, retrieve all his data from the Mexican computer and be back in business within minutes.

So attractive was this technology that in July of 1990, a bookmakers' convention was held at the Hotel San Remo in Las Vegas to demonstrate the system. What the dozen bookies, including Monteleone, did not know was that the technician who helped demonstrate the computer and who was to be responsible for installing and maintaining the computers in the New York area, was actually a Westchester County D.A.'s investigator who had infiltrated the operation. The conventioneers were also unaware that the entire seminar demonstrating the computer system was videotaped in cooperation with the Las Vegas Police Department's intelligence unit for use as evidence in one of the conspiracy counts of the indictment.

Monteleone, confident he was bringing bookmaking into the twenty-first century, purchased and had installed one of the computers in an Ardsley location for use in his own operation. He was unaware that the technician doing the installation was a D.A.'s investigator. He was also unaware that, rather than the Mexican computer being the safe haven for all his gambling records, the computer was, in fact, being down loaded (Pursuant to Court Order), into a computer in the Westchester County D.A.'s Office in White Plains. Those records represent several counts in the present indictment.

In October of 1990 D.A.'s investigators executed several search warrants at locations used by the Monteleone operation. Gambling records and approximately $30,000 in cash were seized at that time. Immediately Monteleone contacted the "technician" (investigator) and asked him to remove

the computer from the Ardsley location "before the cops found it." He obliged. The computer is now being held as evidence at the Courthouse in White Plains. The records electronically seized show over $4.5 million in bets for the period July 30 through August 28, 1990.

Honorable Carl A. Vergari
District Attorney
Westchester County, New York

NARCOTICS

"Almost two-thirds of all court orders for surveillance are used to fight the war on drugs, and electronic surveillance has been critical in identifying and then dismantling major drug trafficking organizations. Although the benefits of these operations are difficult to quantify, their impact on the economy and people's lives is potentially enormous. In 1988, the Public Health Service estimated the health, labor, and crime costs of drug abuse at $58.3 billion [7]. The FBI estimates the war on drugs and its continuing legacy of violent street crime in the form of near daily drive-by murders would be substantially, if not totally, lost if law enforcement were to lose its capability for electronic surveillance."[1]

Kingpin Busted in Four State Cocaine and Heroin Distribution Ring

A recent investigation by the Baltimore State's Attorney and the Baltimore City Police Department focused on a large cocaine and heroin distribution organization. The investigation revealed that the sources of supply for the cocaine and heroin were located in the states of New York, Florida, and California. There was no informant who knew the sources of supply. Further, surveillance could not be maintained by a local police department over a four state area. The only avenue of investigation of all of the co-conspirators was a wiretap. As a result of several wiretaps on residential and cellular phones, three sources of supply for the cocaine and heroin were identified and arrested along with the entire criminal organization in Baltimore.

As a result of the wiretaps and further investigation, evidence in federal court revealed an organization which distributed in excess of 300 kilograms of cocaine in the Baltimore metropolitan area. The kingpin is presently serving life without parole in the federal system. This type of investigation and eventual outcome would have been impossible without the use of wiretaps.

Fentanyl Induced Deaths of Young Adults Halted

In another recent Baltimore City Police Department investigation, it was determined that a drug known as fentanyl had entered the Baltimore Metropolitan area causing death of numerous young adults. It was learned that fentanyl was a controlled substance 100 times more powerful than heroin and was being sold in the Baltimore area under the trade name of China White. Again, normal investigative procedures revealed no information in reference to the source of supply. Due to a wiretap being executed on a local heroin dealer, however, it was learned that this heroin orga-

[1] Denning, Dorothy E., *Communications from the ACM*, March 1993, Vol. 36, No. 3, page 29.

nization was responsible for the smuggling of the fentanyl from the State of New York. The source of the fentanyl was identified and arrested and the heroin and fentanyl distribution organization in the Baltimore area was dismantled. Several individuals have been charged with the deaths resulting from the fentanyl and drug trafficking charges. The cases are pending in both state and federal courts. Further, the drug fentanyl has not been seen in the Baltimore metropolitan area since the above arrest based on the utilization of the wiretaps.

Present investigations into the trafficking of cocaine and heroin in the Baltimore metropolitan area are revealing that the sources of supply are in the states of Florida, New York, Pennsylvania, and California. These investigations, without the use of wiretaps, would only result in the arrest of local retail drug offenders and would not do anything to address the sources of supply.

NOTE: Thorough and effective drug prosecution in the 1990s and beyond will require continued usage of court authorized electronic surveillance. In my professional opinion and based on the experience of my staff, even slight disruption in the access to any and all advanced telephone systems would significantly impair law enforcement's ability to thoroughly investigate drug offenses. In the mid-Atlantic region, as in other jurisdictions, drug distribution organizations are becoming more sophisticated and the majority of the drug smuggling organizations have inter-jurisdictional, inter-state and even international connections and sources of supply. As a result, the conventional investigative techniques such as surveillance, undercover purchases, and the use of informants are becoming increasingly limited as a means to obtain the evidence necessary for the prosecution of the sources of supply without the use of electronic surveillance, which includes both pen registers and wiretaps.

Honorable Stuart O. Simms
State's Attorney
Baltimore, Maryland

Interceptions Uncover Importation of 2,600 Kilos of Cocaine; Seventy Defendants

In the past year, the Philadelphia District Attorney's Office has conducted three separate investigations of major drug distribution networks in which fourteen court ordered interceptions of wire, oral and electronic communications were utilized to intercept criminal conversations and communications on telephones, electronic paging devices and mobile cellular telephones. In each of these investigations, informants and undercover officers were only able to obtain the confidence of and conduct business with mid-level dealers in these distribution networks. The use of electronic surveillance enabled this office to uncover the full extent of these conspiracies as well as to identify their sources of drugs in New York, Miami, Houston, and Cali, Colombia. These investigations have resulted in the arrest of seventy defendants, the seizure of over two hundred kilograms of cocaine, and the confiscation of over two million dollars in assets. The confiscation of records from one of these groups, the "Jude Patrick Thomas" organization, detailed the importation to Philadelphia of 2,600 kilograms of cocaine over an eighteen month period.

The prospect that such criminal groups will be allowed to poison the poor of our cities with impunity is a virtual reality should law enforcement's ability to intercept telecommunications be curtailed.

NOTE: Simply stated, in today's fast paced technological society, electronic surveillance is the eyes and ears of law enforcement. The inability of law enforcement to effectively utilize electronic surveillance will make it virtually impossible to successfully investigate and prosecute organized crime, drug trafficking and official corruption.

As you are well aware, complex criminal conspiracies are by their very nature clandestine affairs, not spectator sport. The identities of conspirators, the nature and mechanics of their illicit enterprise and their innermost thoughts and communications are not for public scrutiny. Yet the conversion of telecommunications to a digital system without preserving law enforcement's ability to intercept conversations is tantamount to giving law enforcement a cheap seat in the bleachers, with only a far removed glimpse of the action.

The use of electronic surveillance has made it possible to penetrate the inner sanctum of criminal conspiracies. Informants and undercover police officers are seldom able to infiltrate the upper echelon of these groups or flush out the true scope of the conspiracy. Only by utilizing electronic surveillance has law enforcement been able to obtain evidence that could not otherwise be gathered and convict defendants with their own words.

Honorable Lynne Abraham
District Attorney
Philadelphia, Pennsylvania

Five Police Officers Busted for Cocaine Distribution

On May 7 of 1992, a five month narcotic investigation utilized at least 21 court ordered wiretaps and registers to dismantle a metropolitan New York conspiracy to sell cocaine. Of the more than 45 defendants charged, five were New York Police Officers who were identified and traced solely through their telephonic communications while dealing drugs. Without the ability to obtain electronic surveillance orders and effectively implement them we would have been unable to bring these malefactors to justice. Obviously, if the defendants' telephone systems incorporated technology which limited law enforcement's ability to intercept, all five of these drug dealers would still be actively selling cocaine while continuing to work as police officers.

1,777 Pounds of Cocaine Confiscated

In December 1989 a team of the Suffolk County District Attorney's investigators, police and Drug Enforcement Administration (D.E.A.) agents concluded a year long investigation with the arrest of nine individuals and the confiscation of 1,777 pounds of cocaine in what was the largest seizure ever in Suffolk County. Three U.S. citizens and six Colombian nationals were arrested in connection with a cocaine smuggling ring that stretched from Colombia through Guatemala, Mexico, Texas, Georgia, and Ronkonkoma, New York. The case was developed primarily through elec-

tronic surveillance and culminated with the interception of a communication that the ring leader Richard Espinosa would arrive at the Long Island warehouse at a designated date and time. The arrest ultimately led to the seizure of an additional 700 pounds of cocaine in Georgia, as well as a forfeiture in excess of $2 million. The cornerstone of this investigation was a series of electronic surveillance orders without which the case could never have been made.

NOTE: Without the ability to intercept communications we would be unable to arrest and convict those sophisticated individuals who control illegal activities in organized crime, including gambling, extortion, robbery, burglary, and the distribution of controlled substances. The proliferation and improvement of pagers or "beepers", cellular phones, and the like has greatly enhanced organized crime's ability to communicate and coordinate their activities.

Honorable James M. Catterson, Jr.
District Attorney
Suffolk County, New York