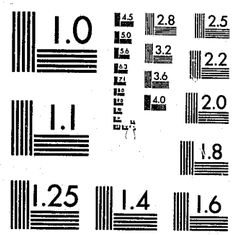
If you have issues viewing or accessing this file contact us at NCJRS.gov.

National Criminal Justice Reference Service

ncjrs

This microfiche was produced from documents received for inclusion in the NCJRS data base. Since NCJRS cannot exercise control over the physical condition of the documents submitted, the individual frame quality will vary. The resolution chart on this frame may be used to evaluate the document quality.



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Microfilming procedures used to create this fiche comply with the standards set forth in 41CFR 101-11.504.

Points of view or opinions stated in this document are those of the author(s) and do not represent the official position or policies of the U. S. Department of Justice.

National Institute of Justice
United States Department of Justice
Washington, D.C. 20531

7/27/83

WIRETAPPING

A REPORT TO THE HAWAII STATE LEGISLATURE

86469

BY THE
HAWAII COMMISSION ON CRIME
State Capitol
Honolulu, Hawaii 96813

JANUARY 1978

PREFACE TO SECOND PRINTING

After the first printing of this report, the 1978 Hawaii Legislature passed a statute authorizing court-ordered wiretapping. The statute enacted was nearly identical to the model statute contained in Appendix I and described in Chapter IV of this report. The few changes made by the Legislature are discussed in Addendum to Chapter VI.

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~copyrighted~~ material has been granted by
Hawaii Crime Commission

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~copyright~~ owner.

NCJRS
NOV 29 1982
ACQUISITIONS

This report is respectfully submitted to the Legislature, State of Hawaii, pursuant to Act 16, First Special Session, Ninth Legislature, State of Hawaii, 1977.

NELSON K. DOI
Chairman
Hawaii Commission on Crime

Commission Members

RAFAEL ACOBA
GENE ALBANO
JOHN BECK
MAGGIE BUNSON
A. VAN HORN DIAMOND
ALWYN KAKUDA
THOMAS OSHIRO
BORICK PEROFF
NAPUA STEVENS POIRE
ANSON REGO
FRANK WHITE, JR.

Hikaru Kerns
Director

James T. Countiss
Legal Counsel

Edward J. Hitchcock
Chief Investigator

ACKNOWLEDGEMENT

With grateful acknowledgement of the assistance of Robert Miller, John Kumabe, John Bassford, Lynn Leong, Susan Flair and Julie Chiya from the Lt. Governor's Office; Carole Richilieu-Ching and Gaylord Tom, law students at the University of Hawaii; and numerous other people, without whose assistance this report would not have been possible.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION TO ELECTRONIC EAVESDROPPING

Wiretapping has long been used by law enforcement officials as an investigative tool. It is not an ordinary tool, in that there are certain potential dangers that accompany any benefits derived from its use. The difficulty in deciding whether to adopt a wiretapping statute is that, in spite of many years of controversy, the precise kind and degree of the potential dangers and benefits of wiretapping have not been clearly established.

On one side of the issue are those whose primary concern is the protection of civil liberties, in particular the right of privacy. Justice Holmes called wiretapping a "dirty business," because of the peculiar "peeping tom" nature of electronic eavesdropping. It is possible for investigators to learn the most intimate and sacred details of people's lives, and such knowledge carries with it an immeasurable power to cause feelings of shame, degradation and insecurity. Though the right of privacy is not expressly mentioned in the Bill of Rights, it is accepted as a natural derivative of the constitutional rights that are clearly stated. The abhorrence that civil libertarians feel toward wiretapping has been enhanced by recently documented cases of illegal and abusive use.

Then there are the law enforcement officials and others who are primarily concerned about the threat posed by crime, especially organized crime. Just as the need for effective investigation of murder and other major crimes is said to justify the invasion of privacy inherent in physical searches, it is claimed that wiretapping is indispensable in certain investigations, and that its benefits override, on certain occasions, the individual's right to be free from being overheard in private conversations. If wiretapping succeeds in undermining organized crime, or in preventing serious crimes, it is argued that society ought to have this tool at its disposal.

The Hawaii Commission on Crime held a public hearing on wiretapping on November 22, 1977, at the State Capitol. Sixteen persons testified. In addition, written testimony was submitted by seven persons. The witnesses included representatives of law enforcement and prosecution, State and Federal, Oahu and Neighbor Islands; the academic community at the University of Hawaii; the Legal Aid and Public Defender Offices; the Hawaii Legislature; labor; the telephone company; the Attorney General; the State Judiciary; and the American Civil Liberties Union. At the public hearing there was vigorous discussion both for and against wiretapping and for and against particular provisions of a state wiretap statute. (The transcript of the public hearing is available at the Crime Commission office.)

The Commission held a decision-making meeting on December 15,

1977, and decided to recommend the adoption of a state wiretapping statute by the Legislature. The Commission further decided on the provisions of a model statute designed to allow court-ordered wiretapping while protecting privacy to the fullest extent possible. The model statute was formally adopted by the Commission on January 16, 1978. (A description of that statute is included as Chapter VI of this report. The text of the statute is in Appendix I.)

The purpose of this report is to provide information that may be helpful in determining the desirability of a state wiretapping law and, if it is desirable, to offer for the Legislature's consideration a model statute that incorporates provisions that have won a measure of support from both civil libertarians and law enforcement officials.

The report will briefly examine the existing laws in Hawaii which prohibit court-ordered wiretapping; describe the state of the art of wiretapping; discuss the constitutional limitations on wiretapping; describe the Federal wiretap statute, which has served as a model for most state wiretap statutes; examine state statutes which differ from and provide alternatives to the Federal model; attempt to assess the effectiveness of wiretapping as a tool to fight crime; and, finally, present and discuss the provisions of a model statute.

DEFINITIONS

It should be noted that "wiretapping" is technically the interception of telephone or other wire communications by a third party using electronic or mechanical devices. But in this report wiretapping will also include "bugging." Bugging is the interception of conversations other than telephone or wire communications by use of a device which transmits or records what is said. The term "electronic surveillance" generally means the use of electronic devices to gather information about what is happening and specifically includes wiretapping and bugging.

In this report, wiretapping will be used generally to mean the interception of both wire and private spoken conversations by electronic or mechanical devices. Wiretapping, including bugging, authorized by a court order is usually referred to as "court-ordered wiretapping." In order to distinguish between wiretapping by court order and wiretapping with the consent of a party(s) to the conversation, the latter will be referred to as "consensual wiretapping."

CURRENT LAW

Hawaii law generally prohibits wiretapping, including bugging, by both private persons and State law enforcement officials.[1] However, wiretapping with the consent of one party to the conversation is

allowed except that bugging requires the consent of all persons entitled to privacy in the place to be bugged. In addition, persons may listen to telephone conversations using their own extension phones or party lines.

Wiretapping, except when authorized by law or in the execution of a public duty, is considered "Violation of Privacy," a misdemeanor punishable by a maximum sentence of one year in jail and a $1,000 fine. Present Hawaii law does not allow state law enforcement officials to apply for a court order authorizing wiretapping. Bills which would have allowed Hawaii state law enforcement officials to apply for court-ordered wiretaps were introduced in the Hawaii Legislature during the 1975, 1976, and 1977 sessions. These bills like most other state statutes were modeled after the Federal wiretap statute.

Federal law allows court-ordered wiretapping by Federal law enforcement officials, such as the FBI. Federal law also allows wiretapping and bugging with the consent of a party to the conversation. The Federal law also authorizes states to enact state laws allowing court-ordered wiretapping.

Twenty-four states currently have statutes which allow court-ordered wiretapping. Most state statutes are modeled after the Federal statute, but some protect privacy more than the Federal statute.

FOOTNOTE

CHAPTER I - INTRODUCTION TO ELECTRONIC EAVESDROPPING

[1]Hawaii Revised Statutes, §711-1111 (1976).

CHAPTER II

CONSTITUTIONAL LIMITATIONS ON WIRETAPPING

Wiretapping and wiretapping statutes are limited by both the United States and Hawaii Constitutions. However, wiretapping was not always thought to be regulated by the U. S. Constitution.

I. HISTORY OF THE CONSTITUTIONAL CONTROLS ON WIRETAPPING[1]

The interception of spoken conversations by a person not a party to the conversation is as old as history itself. The common law of England, on which American law is based, recognized eavesdropping as a public nuisance. The use of electronic or mechanical devices to eavesdrop became common in the United States during the Civil War when opposing forces tapped telegraph lines for military intelligence. There was no uniform reaction to the practice at that time, although some states did prohibit the practice. California enacted a statute in 1862 prohibiting wiretapping of telegraph lines.

With the rapid growth of the telephone system, however, the problem could not be ignored. The New York State Legislature found in 1916 that the local police had been tapping telephone lines, although the practice was prohibited by State law. During World War I, Federal laws were passed prohibiting wiretapping in order to insure the

protection of government secrets. However, these laws were limited to the duration of the war and shortly thereafter wiretapping was again allowed. During the 1920's and early 1930's, the Federal Bureau of Prohibition found the practice of wiretapping useful in apprehending bootleggers.

The Supreme Court first considered the legality of wiretapping in the case of Olmstead v. United States in 1928.[2] The Court decided that the United States Constitution's Fourth Amendment ban against unreasonable searches and seizures was not violated by wiretapping.[3] The reasoning of the Court was that there was no physical invasion of a home or office by wiretapping and that there was no seizure of tangible items.[4] The Court also concluded that the Fifth Amendment ban against compulsory self-incrimination was not violated because no person was being "compelled" or forced to be a witness against himself.[5]

The Supreme Court decided in 1942 in Goldman v. United States that bugging, like wiretapping, did not violate the Fourth Amendment prohibition against unreasonable searches and seizures.[6] The reasoning behind this decision was the same as that in Olmstead. The bugging did not involve a physical trespass into Goldman's office and there was no seizure of tangible items from the office.[7]

In 1934, Congress passed Section 605 of the Communications Act of 1934 prohibiting the interception and divulgence of wire communica-

tions. Thus, although the Constitution allowed wiretapping, a Federal statute prohibited it. Three years later the Supreme Court ruled that evidence from a wiretap that violated Section 605 of the Federal Communications Act of 1934 could not be used as evidence at a Federal criminal trial.[8] In 1939, the Court also ruled that evidence discovered as a result of information gained by illegal wiretapping could not be used.[9] The Department of Justice, however, interpreted Section 605 to mean that Federal agents could not both intercept and divulge in court the contents of wire communications. It continued to wiretap for strategic information until 1940, when the Attorney General adopted a policy prohibiting wiretapping. During World War II, however, President Roosevelt did use wiretapping extensively to check the activities of foreign agents.

Also, consensual exceptions to Section 605 of the Federal Communications Act were recognized. In On Lee v. United States, the Court found that a government informant could transmit conversations through a device hidden on his body because the defendant, by voluntarily conversing with the informant, consented to the interception of the conversation by that informant.[10]

In 1963, the Supreme Court clearly stated that verbal evidence as well as tangible items are protected from unreasonable search and seizure.[11] Finally in 1967, two Supreme Court cases finally changed the law of wiretapping and electronic eavesdropping, deciding that

wiretapping was a search and seizure that must not be unreasonable. In Katz v. United States, the Court abandoned the concept of trespassory invasion and moved toward an invasion of privacy concept.[12] In the Katz case, FBI agents had attached a bug to the exterior of a phone booth used by the defendant.[13] The Court did not rely on the theory of trespassory invasion, but instead declared that the Fourth Amendment protects a person's reasonable expectation of privacy whether or not a physical trespass is involved.[14] The Court held that wiretapping was a search and seizure and that a court order was required before it was reasonable.[15]

In Berger v. New York, the Supreme Court found that a New York statute authorizing court-ordered wiretapping was constitutionally deficient in not providing Fourth Amendment safeguards.[16] Among the absent safeguards were a failure to require facts rather than conclusions to support the issuance of a wiretap order; a particular description of the conversations to be seized and of the crime that had been or was being committed; an explanation of why no prior notice of the search was given to those persons whose privacy had been invaded; and other limitations on the officers executing the order.[17] Finally the constitutionality of consensual wiretapping and bugging was clearly established in United States v. White, decided in 1971.[18]

The Katz and Berger decisions made clear that wiretapping was a search and seizure subject to Fourth Amendment controls and formed the basis for the present constitutional law of wiretapping.

II. THE LAW OF SEARCH AND SEIZURE

Both the United States and Hawaii Constitutions prohibit unreasonable searches and seizures by government officials and require warrants to be issued only upon probable cause established by sworn facts.* In addition, both the United States and Hawaii Constitutions prohibit unreasonable invasions of an individual's right of privacy.[19] Hawaii's Constitution expressly includes the right of privacy while the Federal Constitution does not do so.[20] The right of privacy is implied in the Federal Constitution.[21] Nevertheless, the Federal and the Hawaii rights of privacy are probably the same and each probably is identical to the prohibition against unreasonable searches and seizures for our purposes.**

---

*Fourth Amendment, U. S. Constitution (1791) provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article I, Section 5, Hawaii Constitution (1968) provides:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches, seizures, and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted.

**State v. Pokini, 45 Haw. 295, 309 (1961). It should be noted, however, that the Hawaii Supreme Court could interpret Article I, Section 5, of the Hawaii Constitution to protect privacy even more than the Fourth Amendment to the U. S. Constitution does; State v. Cotton, 55 Haw. 361 (1973); State v. Texeira, 50 Haw. 138 (1967). It is doubtful that Hawaii's Constitution could be interpreted to prohibit

A search occurs when officials look in a place that a person reasonably expects to be private.[22] A seizure occurs when government officials take possession of a person or property including intangible property.[23] Wiretapping is now considered a type of search and seizure, since private conversations are searched for incriminating statements and then seized for use by law enforcement officials.[24] Thus, wiretapping must not be unreasonable and must generally meet the warrant requirements for legal searches and seizures.[25]

THE WARRANT REQUIREMENT

Generally, a search warrant or court order approving a search and seizure must be obtained before any search or seizure is reasonable.[26] However, there are exceptions to the requirement of a search warrant in certain emergency situations where there is danger to persons or the probability of evidence being destroyed or lost and no time exists to obtain a warrant before the search.[27] Some of the exceptions to the warrant requirement are searches incident to arrest, searches of a vehicle for contraband, stop and frisk, and searches while in hot pursuit of an offender.[28] Searches with the consent of a person entitled to privacy in the place to be searched is also an exception to the warrant requirement and to other

---

(cont'd) wiretapping since the language of Article I, Section 5 contemplates the interception of communications pursuant to a warrant particularly describing the communications.

requirements of reasonableness.* The right to be free from unreasonable searches and seizures, like any other constitutional right, may be knowingly and voluntarily waived.[29] Thus, if a person consents to a search, the search is no longer subject to the requirements of the Fourth Amendment.

PROBABLE CAUSE

A court can only issue a warrant after determining that there is (1) probable cause to believe a crime has been or is being committed and (2) probable cause to believe that the place to be searched contains particular evidence of that crime.[30] Stated simply, probable cause is facts which justify a reasonable belief that a crime is being committed and that evidence may be obtained by the search.[31] It is more than just a suspicion or hunch but less than convincing evidence of guilt.[32] The government official requesting the warrant must show the court, by way of affidavit, facts and circumstances which support probable cause as to the crime and existence of the evidence to be seized.[33] The affidavit must set out the facts supporting probable cause, not just a conclusion that probable cause exists or that the official believes there is probable cause.[34]

*Ringel, Searches and Seizures, Arrests and Confessions §167.01, p. 202 (1972). Consent searches are not subject to the requirements of the Fourth Amendment to the U. S. Constitution or Article I, Section 5, of the Hawaii Constitution. Consent searches are not required to satisfy any of the requirements for other searches and seizures.

PARTICULAR DESCRIPTION

The search warrant must describe particularly the person or place to be searched and the things to be seized.[35] Almost any place or any person can be searched as long as there is probable cause to believe that evidence of a crime will be found in the place to be searched. If the search is of a place, then the persons who may be there are not required to be described with particularity in order to search the place except to the extent necessary to describe the place. For example, a description of the owner or occupant of an apartment to be searched may be necessary to accurately describe the apartment. If the search is of a person, then the person must be particularly described.[36] A description of a person as John Doe is not sufficiently particular, although the person's name, if unknown, is not necessary as long as the person is particularly described.[37]

The warrant must also particularly describe the things to be seized.[38] A seizure may be made of any fruits, instrumentalities, or evidence of crime, or contraband, that are particularly described in the warrant.[39] Conversations and recordings of conversations can also be seized when they are fruits, instrumentalities or evidence of crime.[40] Also, what a law officer observes or hears during a search can be seized and is considered evidence which is the product of a search and seizure.[41]

The scope of the search and seizure and, thus, the extent of the invasion of privacy is limited and controlled by the particular description of the person or place to be searched and the items to be seized.[42] A search cannot be conducted of places other than those described in the warrant.[43] Also, the extent of the search is limited by the nature of the items to be seized.[44] For example, if the warrant describes a rifle, then a search of jewelry boxes or other places too small to conceal a rifle would probably be considered outside the legal scope of the search. Only the things particularly described in a search warrant may be seized, with the exception of contraband and other evidence of crime reasonably related to the search which can be seized when they are found in the course of an otherwise legal search.[45]

NOTICE

All other aspects of the search itself must also be reasonable.[46] Generally, notice of a search is required before the search, unless there are exceptional circumstances why notice cannot be given.[47] For example, prior notice of a search for narcotics might result in destruction of the evidence which is sought by the search. Prior notice probably would not be required in this situation.[48] In the case of exceptional circumstances, notice of the search must be given within a reasonable time after the search.[49] Oftentimes the notice is given immediately prior to the entry and search.[50]

PROMPT EXECUTION

The search itself must be conducted within a reasonable time after the warrant is issued.[51] This is intended to make sure that the probable cause that justifies the search is still present at the time the search is conducted.[52] Federal law requires execution of the search warrant within 10 days.[53] Although the Constitution does not expressly state that a warrant must be executed within 10 days, the Constitution requires that searches be reasonable. The Federal rule allowing 10 days is evidence of what Congress thinks is a reasonable time.

DURATION

The duration as well as the scope of the search must be reasonable.[54] The search may be no longer than reasonably necessary to conduct the search.[55] Usually, this means the search must terminate when the things described in the warrant are found.[56] This requirement also limits the extent of the invasion of privacy.

RETURN ON THE SEARCH

Generally, the search warrant and an inventory of items seized must be returned to a judge.[57] The inventory is also required to be given to the person to whom the items belong, upon request.[58]

However, failure to do either of these requirements does not necessarily make the search illegal.[59] The inventory serves as notice to the person(s) whose premises were searched of the fact of the search and seizure and of the things seized.

EFFECT OF ILLEGAL SEARCHES

If a search and seizure is unreasonable and thus in violation of the Constitution, several possible remedies exist. If the judge determines at the time of application for a search warrant that the application is insufficient, he must deny the application.

THE EXCLUSIONARY RULE

If the search has already occurred, generally the evidence can be excluded from a criminal trial and the person whose privacy was invaded may sue for damages.[60] The Constitution prohibits the use of evidence obtained as a result of an unreasonable search at a criminal trial of the person whose privacy was invaded.[61] This is called the exclusionary rule. The Fourth Amendment does not expressly state that evidence obtained in an unreasonable search must be excluded from a criminal trial. However, the United States Supreme Court has determined that exclusion of such evidence is required by the Fourth Amendment to deter law enforcement officers from activity in violation

of the Constitution.[62] The exclusion is not automatic but is accomplished through a motion to suppress the evidence in a criminal trial, which must be made by the defendant or his attorney.[63] If the judge then determines (1) that the search was unreasonable, (2) that the defendant's right to privacy was invaded by the search, and (3) that the evidence sought to be admitted was obtained as a result of the search, the evidence must be excluded.[64] The evidence excluded includes both the actual things seized in the unreasonable search, including what the officers saw and heard during the search and any evidence discovered not only in the search itself but as a result of the evidence obtained in the search.[65]

CIVIL SUIT

The Constitution also allows a civil suit for damages by the person whose privacy was invaded against the law officers who conducted the search.[66] This right also is not expressed in the Fourth Amendment but is allowed by judicial decisions interpreting the Constitution to deter police conduct in violation of the Constitution.[67] This civil suit is similar to and generally governed by rules for other civil suits for damages.[68]

III. WIRETAPPING

Although wiretapping is usually a search because of its very

nature, it must interfere with a person's reasonable expectation of privacy before it is considered a search.[69] The interception of telephone conversations almost always interferes with a person's reasonable expectation of privacy.* However, bugging may or may not invade an expectation of privacy. For example, if the bugging is conducted in a crowded park where conversations could be overheard without the aid of any device, there probably is no reasonable expectation of privacy and, thus, no search.

Since wiretapping is considered a search and seizure, it must be reasonable and, generally, must comply with the rules for all other searches and seizures.[70] However, because wiretapping is different from other types of searches and seizures in that law officers use electronic devices to search and seize conversations over a period of time, there are problems in applying all the requirements of search and seizure to wiretapping.

THE WARRANT REQUIREMENT

Wiretapping requires a court order much like a search warrant.[71] As in other searches and seizures, the purpose of the warrant requirement is to establish judicial control of decisions of law officers to conduct searches and of the limits of the search.[72] As with other searches and seizures, there may be exceptions to the warrant requirement. However, all of the exceptions applicable to ordinary searches and seizures may not apply to wiretapping.[73] Wiretapping may probably be done without a prior court order in an emergency situation where there is no time to obtain a warrant before evidence is lost or destroyed.[74] Probable cause and the other elements of reasonableness would still be required.* There are few court decisions setting the permissible parameters for emergency wiretapping. However, several courts have generally held that Federal and similar state statutes containing a provision allowing emergency wiretaps to be constitutional.[75]

CONSENSUAL WIRETAPPING

In addition neither a wiretap order nor probable cause is necessary for wiretapping with the consent of a party wiretapped.[76] This latter exception is similar to the consent exception for other searches and seizures. In other searches and seizures, consent may be given by any person entitled to possession and control of the thing(s) to be searched.[77] The consent of all persons who have a right to possession or control of the thing(s) searched is not necessary.[78]

*Thus, the Federal Wiretapping Statute prohibits all unauthorized interception of wire (telephone) communications but prohibits unauthorized interception of oral communication only when it is intended to be private. See 18 U.S.C. §§2510(1) and (2) and 2511 (1970).

*See, e.g., Carolle v. U.S., 267 U.S. 132, 136 (1925). A warrantless search of an automobile for contraband was found unreasonable because there was no probable cause.

Thus, in consensual wiretaps, only the consent of one party to the conversation is required.[79]

The reason for the consent exception is that a person takes the risk that others who share premises or conversations and thus have knowledge of the contents of the premises or conversations may disclose the contents to others.[80] Thus, it is reasoned, a person has no expectation of privacy in shared premises or shared conversation beyond the probability that the person sharing the knowledge will choose not to disclose it. This rationale equates disclosure by the trusted person with a search and seizure on the premises or of the conversation by a third party.

The Constitution probably allows wiretapping, without a court order with the consent of any party to the conversation.[81] Generally, other exceptions to the warrant requirement recognized for general searches and seizures do not apply to wiretapping.[82]

PROBABLE CAUSE

Like a search warrant, a wiretap order can only be issued upon probable cause (1) that a particular crime has been, or is being committed and (2) that incriminating statements concerning the particular crime will be made over the lines being tapped or in the place being bugged.[83] Again, as with search warrants, the probable cause

must be established in the application by way of sworn facts as opposed to conclusions of the applicant.[84] The application and order must also describe the specific offense involved.[85]

PARTICULAR DESCRIPTION

As with search warrants, a wiretap application and order must describe particularly the place or persons to be searched and the things to be seized.[86] It is unclear whether wiretapping is a search of a person or of a place. Wiretapping, including bugging, is probably considered a search of a place since the search is focused on a place, is stationery, and is not limited to particular persons.* Thus, the facilities or the place to be wiretapped must be described accurately. It is unclear whether the Constitution requires the person to be intercepted to be described, beyond any description necessary to particularly describe the facilities or place to be wiretapped or other conversations to be seized. For example, a description of the person leasing the telephone or apartment to be wiretapped may be necessary to particularly describe the place to be searched. Also, a description of the person may be necessary to establish probable cause that a crime is being committed. However,

*Berger v. New York appears to treat wiretapping as a search of a place. See 388 U.S. at 56. However, the New York statute provided for the naming of persons to be intercepted, so that the court did not reach the question of whether it is a search of a person or place. See 388 U.S. at 59.

whether or not a person is particularly described, conversations of persons other than the person(s) described can be intercepted.[87]

As with search warrants, the purpose of requiring particular descriptions of the persons or place to be wiretapped is to limit the scope of the search and, thus, limit the extent of the invasion of privacy.[88] Requiring only a description of the room to be bugged and the telephone to be wiretapped has been criticized since it does not limit the scope of the search very much.[89] Conversations of anyone in the bugged room or using the wiretapped telephone are intercepted. In other searches a law enforcement official cannot remain in a house for long periods of time and indiscriminately observe or search everyone who enters the house. In addition, allowing the search of any person's conversations may establish guilt by association. Anyone communicating with a person thought to be committing a crime or at a place where a crime is being committed may have their conversations searched.

The Constitution also requires that an order particularly describe the things to be seized.[90] In the case of wiretapping, the things to be seized are conversations that have not yet occurred. A wiretapping order is required to particularly describe the type of conversations to be seized, since it is impossible to accurately describe future conversations.[91] This requirement of particularity may limit the scope of the search and seizure more effectively than the requirement of a description of the place or facilities to be wiretapped.[92]

MINIMIZATION

In other searches, the search must be limited to places where the items to be seized could be hidden.[93] In wiretapping, only conversations in which the type of communications described in the order are likely to occur may be searched and seized.[94] For example, enforcement officers listening to and recording conversations on a crime figure's phone should cease monitoring and recording when the babysitter calls her boyfriend. This is called minimization and is intended to minimize the invasion of privacy resulting from wiretapping.[95] Minimization has been criticized because it is difficult to determine in advance what conversations are likely to result in incriminating statements related to the described offense.[96] For example, a crime figure's call to his wife, mistress, or mother may or may not result in a discussion of criminal activities.

Generally, the seizure of incriminating conversations other than the type described in the application and court order should be allowed as long as the conversation appeared at the time the interception is occurring to be likely to contain statements of the type described in the application and order.[97]

NOTICE

As with other searches, prior notice of the search, or circum-

stances why prior notice cannot be given, is required for wiretapping.[98] Some courts feel that the failure or the danger of investigative methods other than wiretapping is considered exigent circumstances why prior notice cannot be given.[99] The nature of wiretapping is such that exigent circumstances why prior notice may not be given are probably present in every case. In the same way that prior notice may result in the destruction of evidence in searches for drugs, incriminating statements will almost certainly not occur if prior notice of a wiretap is given.

As in other searches, notice must be given within a reasonable time after the search if it cannot be given before.[100] In the case of wiretapping, most courts feel that 90 days after the termination of the wiretap is a reasonable time.[101]

PROMPT EXECUTION AND DURATION

Like other searches, a wiretap order must be promptly executed or begun, and the duration of the search must not be unreasonable.[102] Unlike other searches, wiretaps are of a continuing nature lasting over a period of time. Since the duration of the search in wiretapping continues over a period of time, there is a problem of ensuring the existence of probable cause throughout the duration of the search.[103] In other searches this problem is solved by prompt execution. In wiretapping the problem must be solved by limiting the

duration of the search and requiring proof of probable cause before the wiretap can continue further.[104]

The U. S. Supreme Court has decided that 60 days is an unreasonable duration and that wiretaps, like other searches, cannot continue after the things to be seized have been found and seized.[105] Thus, wiretaps like other searches must automatically terminate when the type of conversation described in the order has been seized.[106] Just as it is difficult to accurately describe in advance the conversations to be seized, it is difficult to determine whether a particular conversation seized is the type of conversation described in the order which is the ultimate object of the search. The conversation intercepted may be incriminating and may be of the type described but may not be the convincing proof of guilt which is sought by the wiretap. Thus, the requirement of automatic termination is both difficult to apply and to enforce.

RETURN ON THE WIRETAP

Finally, the wiretap order, like other searches, must be returned to a judge who has control over the wiretap.[107] Usually, a return includes an inventory listing the things seized in the search.[108] Also a copy of the inventory and search warrant is usually given to the person whose place is searched or whose things are seized within a reasonable time after the search.[109] It is not clear whether the

Constitution requires this in the case of wiretapping, although this may be considered necessary to make wiretapping a reasonable invasion of privacy. Additionally, all other aspects of a wiretap must be reasonable.[110]

THE EXCLUSIONARY RULE AND CIVIL SUIT

Like other unreasonable searches and seizures, evidence obtained as a result of an unreasonable wiretap is excluded from a criminal prosecution and a civil suit may be brought for damages suffered as a result of the wiretap.[111]

IV. CONSTITUTIONAL LIMITATIONS AND THE FEDERAL WIRETAP STATUTE

The Federal wiretap statute generally incorporates the requirements of the U. S. Constitution concerning the use of wiretaps. Although the United States Supreme Court has not examined the constitutionality of all the provisions of the Federal statute, numerous other courts have upheld its constitutionality.[112]

V. CONCLUSION

Although all the constitutional limits on wiretapping have not yet been decided, it is clear that wiretapping must generally meet the reasonableness requirements for other types of searches and seizures.

In particular, wiretap orders can only be issued upon probable cause that a particular crime is being or has been committed and that incriminating statements concerning that crime will be intercepted through the facilities or at the place to be wiretapped. In addition the existence of the probable cause must be established by sworn facts. Both applications and orders must describe particularly the specific offense involved, the facilities or the place to be wiretapped, and the type of communications to be intercepted. The order must be promptly executed. The reasons for not giving prior notice of the wiretap should be stated. The duration of the wiretap must not be unreasonable. The wiretap must automatically terminate when the conversations described have been seized. There must also be judicial control of the execution of the wiretap and a return to a judge.

FOOTNOTES

CHAPTER II - CONSTITUTIONAL LIMITATIONS ON WIRETAPPING

[1]This brief history is taken from the opinion of Justice Clark in Berger v. New York, 388 U.S. 41, 45-53 (1967); Carr, Electronic Surveillance §§1.02 and 1.03 (1977); and National Wiretap Commission, Commission Studies, pp. 2-5 (1976).

[2]277 U.S. 438 (1928).

[3]Ibid., p. 466.

[4]Ibid., pp. 464-466.

[5]Ibid., p. 462.

[6]316 U.S. 129 (1942).

[7]Ibid., pp. 135-136.

[8]Nardone v. U.S., 302 U.S. 379 (1937) (known as Nardone I).

[9]Nardone v. U.S., 308 U.S. 338 (1939) (known as Nardone II).

[10]343 U.S. 747 (1952).

[11]Wong Sun v. U.S., 371 U.S. 471 (1963).

[12]389 U.S. 347, 350-353 (1967).

[13]Ibid., p. 348.

[14]Ibid., pp. 350-353.

[15]Ibid.

[16]388 U.S. 41 (1967).

[17]Ibid., pp. 58-59.

[18]401 U.S. 745, reh. den. 402 U.S. 990 (1971).

[19]Ibid.

[20]Ibid.

[21]See e.g., Berger v. New York, 388 U.S. at 53.

[22]See e.g., Katz v. U.S., 389 U.S. at 351-53.

[23]Ibid., p. 353.

[24]Katz v. U.S., 389 U.S. at 351-53; Berger v. New York, 388 U.S. at 53-54.

[25]Katz v. U.S., supra; Berger v. New York, supra.

[26]Ringel, Searches and Seizures, Arrests and Confessions §167.01, p. 202 (1972), citing Katz v. U.S., 389 U.S. at 357.

[27]Ringel, op. cit., §167.01, p. 202, citing Katz v. U.S., 389 U.S. at 357, note 19.

[28]Ringel, op. cit., §167.01, pp. 202-203.

[29]Ibid., §230, p.288.

[30]Ibid., §171.01, p. 208 and §183, p. 231.

[31]Ibid., §170, pp. 206-207, quoting Stacey v. Emery, 97 U.S. 642, 645 (1878).

[32]Ringel, op. cit., §170, p. 206, quoting Agnello v. U.S., 269 U.S. 20, 33 (1925).

[33]Fourth Amendment, U.S. Constitution; Art. I, Sec. 5, Hawaii Constitution.

[34]Ringel, op. cit., §170, p. 207, citing Aguilar v. Texas, 378 U.S. 108 (1964).

[35]Fourth Amendment, U.S. Constitution; Art. I, Sec. 5, Hawaii Constitution; Ringel, op. cit., §183.02, p. 236 and §189, p. 241.

[36]Ringel, op. cit., §189, p. 241.

[37]Ibid., citing Keiningham v. U.S., 287 F.2d. 126 (1960).

[38]Ibid., §183.02, p. 236, citing Marron v. U.S., 275 U.S. 192 (1927).

[39]Ibid., §171.01, p. 208, citing Aguilar v. Texas, 378 U.S. 108 (1964).

[40] Ibid., §183.01, p. 235.

[41] Ibid., §320, p. 408, citing Hoffa v. U.S. 385 U.S. 293 (1966).

[42] Carr, op. cit., §2.05[a], p. 34.

[43] Ringel, op. cit., §189, p. 241.

[44] Carr, op. cit., §2.05[a], p.34.

[45] Ringel, op. cit., §183.02, pp. 236-37 and §188, pp. 240-41.

[46] Ibid., §167.01, p. 202. See generally, Ibid., §§190-198.

[47] Ibid., §194, p. 246, citing Ker v. California, 374 U.S. 23 (1962).

[48] Ringel, op. cit., §194, p. 246 and §194.01, p. 246.

[49] Carr, op. cit., §2.05 [2][d], pp. 40-41.

[50] Ringel, op. cit., §194.01, p. 246.

[51] Ibid., §193, p. 245.

[52] Ibid., §170, p. 207, citing Sgro v. U.S., 287 U.S. 206 (1932).

[53] Ringel, op. cit., §198, p. 251.

[54] Ibid., §195.02, pp. 248-49.

[55] Ibid.

[56] Ibid.

[57] Ibid., §196, p. 249.

[58] Ibid.

[59] Ibid., §198, p. 251 and §199, pp. 251-252, citing Evans v. U.S., 242 F.2d 534 (1957)

[60] Ringel, op. cit., §10, pp. 18-19. See also Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971).

[61] Ringel, op. cit., §10, pp. 18-19.

[62] See, e.g., Mapp v. Ohio, 367 U.S. 643, (1961); Weeks v. U.S., 232 U.S. 383, (1914).

[63] Ringel, op. cit., §342, p. 440 and §347, p. 447.

[64] Ibid., §346, pp. 444-446.

[65] See, e.g., Wong Sun v. U.S., 371 U.S. 471 (1963).

[66] Bivens v. Six Unknown Named Agents, supra.

[67] Ibid., pp. 396-397.

[68] See generally, Ibid., pp. 390-397.

[69] Katz v. U.S., 389 U.S. at 351-52; Carr, op. cit., §1.03[5], p. 15.

[70] Berger v. New York, supra.; Katz v. U.S., supra.

[71] Katz v. U.S., 389 U.S. at 358-359.

[72] Ibid.

[73] Ibid., p. 359.

[74] Carr, op. cit., §3.07[1], pp. 116 and 118.

[75] Ibid., §2.05[2], p. 33 and cases cited in notes 116-119. See also Ibid., notes 122 and 124, p. 34.

[76] U.S. v. White, 401 U.S. 745, 753-754; Carr, op. cit., §3.05[2], pp. 91-92.

[77] Ringel, op. cit., §232, pp. 290-292.

[78] Ibid., p. 292.

[79] Ibid., §3.05[2], pp. 91-92 and cases cited in note 324, p. 92.

[80] Ibid., §3.05[2], p. 92.

[81] U.S. v. White, supra.

[82] Katz v. U.S., 389 U.S. at 359 (dicta).

[83] Berger v. New York, 388 U.S. at 54-55.

[84] Ibid., p. 57.

[85] Ibid., pp. 57-59; Carr, op. cit., §2.05[a] and note 132, p. 34.

[86] Berger v. New York, 388 U.S. at 55-59; Carr, op. cit., §2.05[a] and notes 130 and 134, p. 34.

[87] Carr, op. cit., §2.05[2][b] and notes 153-154, p. 37.

[88] Berger v. New York, 388 U.S. at 57-59; Carr, op. cit., §2.05[a][2], p. 34.

[89] Carr, op. cit., §2.05[a][2], and note 155, p. 34.

[90] Fourth Amendment, U.S. Constitution; Art. I, Sec. 5, Hawaii Constitution.

[91] Berger v. New York, 388 U.S. at 57-59; Carr, op. cit., §2.05[a][2] and notes 130, 134, p. 34.

[92] See Berger v. New York, 388 U.S. at 57-59; Carr, op. cit., §2.05[a][2] and notes 130, 134, p. 34.

[93] Ringel, op. cit., §183.02, p. 236.

[94] Berger v. New York, 388 U.S. at 57-59.

[95] National Wiretap Commission, Commission Studies, pp. 14-15.

[96] Carr, op. cit., §5.07[1], pp. 257-258, and §5.07[2], p. 258.

[97] Ibid., §5.09, pp. 269-270 and §5.09[1], pp. 270-273.

[98] Berger v. New York, 388 U.S. at 60.

[99] Carr, op. cit., §2.05[2][d], and notes 178-183 and 188, pp. 40-41.

[100] Ibid., §2.05[2][d][ii], pp. 41-42.

[101] Ibid., §2.05[2][d], notes 182, 183, 188, p. 41.

[102] Berger v. New York, 388 U.S. at 59-60.

[103] Ibid., p. 59; Carr, op. cit., §2.05[2][c], pp. 38-40.

[104] Berger v. New York, 388 U.S. at 59.

[105] Ibid., pp. 59-60.

[106] Ibid.

[107] Ibid., p. 60.

[108] Carr, op. cit., §2.05[2][d], p. 42.

[109] Ibid.

[110] Ibid., §§5.01-5.13, pp. 241-292.

[111] Berger v. New York, 388 U.S. at 1048; Carr, op. cit., §804[1], p. 495; Ringel, op. cit., §326, p. 419.

[112] Carr, op. cit., §2.05[2] and notes 116-119, 122 and 124, pp. 33-34.

CHAPTER III

THE FEDERAL WIRETAP STATUTE

I. INTRODUCTION

There has been a Federal statute that allows court-ordered wiretapping by Federal law enforcement officials since 1968. This law, which is often referred to as Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[1] was written to accomplish two primary purposes. The law is intended, first, to provide a means of combatting organized crime[2] and, second, to protect the privacy of spoken communications.[3] The Federal law accomplishes these somewhat inconsistent purposes by defining the circumstances under which the interception by electronic or mechanical devices of private spoken communications can be authorized, and prohibiting other unauthorized interceptions of spoken communications.[4] Generally, Title III allows the interception of conversations by Federal law enforcement officers pursuant to a court order which sets forth strict limits on the operation and use of the wiretap.[5] The law prohibits all other mechanical or electronic interception of such conversations, without the consent of a party to the conversation.[6] The Federal law also establishes minimum standards for state authorization of court-ordered wiretapping.[7]

II. SCOPE

PRIVATE SPOKEN COMMUNICATIONS

Title III applies to and prohibits all interceptions by devices of "wire or oral communications" with certain specified exceptions.[8] Title III was intended to be "comprehensive," and covers both intrastate and interstate wire communications. In passing the law, Congress noted that in this country these communications are "inextricably interwoven."[9] Title III also governs non-wire oral communications made with a reasonable expectation that it is not subject to being intercepted.[10] The subjective intent of the person making the statement or utterance and the place where the communication is uttered, among other circumstances, may be considered in determining whether an expectation of privacy is justified. Thus, Title III generally prohibits, with some exceptions, the interception by any device (other than the ear) of private spoken communication.

Title III provides exceptions for and, thus, allows consensual interceptions; interceptions by use of extension phones or party lines, interception by telephone, telegraph and other communications companies and agencies including the Federal Communications Commission; and interceptions pursuant to court order by Federal or state law.

CONSENSUAL WIRETAPPING

Title III allows any person to intercept conversations if he is a party to the conversation or has the consent of one of the parties to the communication. This type of interception is often called "consensual" interception. A private person may conduct such an interception, as long as his purpose is not "criminal or tortious."[11] The consensual exception is based upon the idea that the law should only protect a person's reasonable expectation of privacy. A person communicating with another person takes the risk that the other person will disclose the contents of the conversation. Since this is so, it is no different if the other person allows someone else to listen, record or transmit the conversation to a third party. Thus, consensual interception does not interfere with a person's reasonable expectation of privacy. This reasoning has been criticized since having your conversation recorded or having an uninvited stranger as an unknown party to your conversation may be considered different than the risk that a friend may later tell in his own words what he remembers of your conversation with him.

BUSINESS NECESSITY WIRETAPPING

Telephone and other communications companies may conduct random monitoring of conversations in order to maintain mechanical and service quality control.[12] Finally, an employee of the Federal

OFFENSES

Court-ordered wiretapping can be used to investigate only those criminal offenses specified in the statute. The offenses were chosen because they were thought to be characteristic of the activities of organized crime.[16] These crimes include, among others, murder, kidnapping, riots, robbery, extortion, bribery, transmission of wagering information, obstruction of justice, interference with commerce by threats or violence, racketeering enterprises, counterfeiting, bankruptcy fraud, dealing in narcotics, and extortionate credit transactions. Any conspiracy to commit any offense listed in the Federal statute is also included.[17]

WHO MAY APPLY

Any Federal official who can investigate or prosecute the crimes listed in the statute may apply for a wiretap order.[18] However, the Attorney General, or a designated Assistant Attorney General, must authorize the application.[19] In practice, a number of law enforcement officials must concur before an application for an interception can be made to a Federal judge. Usually applications are initiated by a Federal law enforcement officer such as an FBI agent in conjunction with a U. S. Attorney. Once the decision is made to apply for a wiretap order, the approval of the heads of both the local U. S. Attorney's Office and the local FBI office is sought. Then the

application is sent to Washington, D. C. with supporting documents for approval by the FBI office and finally forwarded to the Attorney General of the United States. Ultimately, the wiretapping application would need to receive authorization by the U. S. Attorney General or by his "specially designated" Assistant Attorney General. Then the application would be made to a Federal judge for a wiretap order. The legislative history of this section indicates its purpose:

> *This provision centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques. Centralization will avoid the possibility that divergent practices will develop. Should abuses occur, the lines of responsibility lead to an identifiable person. This provision in itself should go a long way toward guaranteeing that no abuses will happen.*[20]

WHO MAY ISSUE ORDERS

Under Title III, the application for interception of a wire or oral communication must be made to a U. S. District Court or a U. S. Court of Appeals judge.[21] According to the legislative history, neutral and detached judicial review will ensure that a proper and fair decision will be made.[22]

WIRETAP ORDERS

The Federal wiretap law sets out very specific requirements for

both wiretap applications and orders. The application for a wiretap order must be in writing and upon oath, usually by affidavit containing the facts supporting the application, and must state the applicant's authority to apply. In addition, the application must state the identity of the law officers involved; sworn facts supporting the application including details of the particular offense committed, being committed, or about to be committed, a particular description of the nature and location of facilities or place of interception; a particular description of the type of communications to be intercepted; the identity of the person committing the offense and being intercepted; and whether other investigative procedures have been tried and failed or why they appear unlikely to succeed or are too dangerous. The application must also give the facts regarding previous applications involving the "same persons, facilities or places"; the period of time for which the interception is to be maintained; and, if the order is not to terminate upon the interception of the incriminating statement, the facts establishing probable cause to believe that additional incriminating statements will be made.[23] The legislative history states that these requirements reflect the constitutional requirements for court-ordered wiretapping established by the U. S. Supreme Court in Berger v. New York and Katz v. United States.[24] Applications for extensions of wiretaps must also state the results of the wiretap or an explanation of the failure to obtain results in addition to satisfying the requirements for an original application, set out above.[25]

The Federal law also specifies what the authorizing judge must determine before he can issue a wiretap order. The issuing judge must determine that there is probable cause to believe that an offense included in the wiretap statute is being, has been, or is about to be committed by an individual. The judge must also determine that there is probable cause to believe that particular communications concerning the offense will be obtained through the wiretap and that normal investigative procedures have failed, appear unlikely to succeed, or are too dangerous. The judge must also determine that there is probable cause to believe the facilities or the place where the interception will be made are being used or are about to be used in the commission of the offense, or are leased to, listed in the name of, or used by the person named in the application and order.[26] According to the legislative history, these requirements are intended to reflect the constitutional standards enunciated in Berger v. New York.[27]

Title III also specifies the required contents of a wiretap order. The order must specify the identity of the person, if known, whose communications are to be intercepted, the nature and location of the facilities or place of interception, the type of communication to be intercepted, the particular offense involved, the agency authorized to intercept, the person authorizing the application, and the maximum duration of the interception including whether the interception automatically terminates when the described communication is obtained.[28]

DURATION

Title III allows interception pursuant to an order for up to 30 days.[29] However, the wiretap should automatically terminate when the incriminating communications described in the application and order are intercepted, unless the order provides for continued interception. Title III allows extensions of up to 30 days each. There is no statutory limit on the number of extensions which may be granted, but a period of extension must also terminate automatically when the specified conversations are intercepted, unless the order provides for continued interception. Orders granting extensions are governed by the same requirements set forth for the original wiretap order.[30]

EMERGENCY WIRETAPS

The Federal law allows emergency wiretaps without prior court order. A wiretap may be initiated in an emergency situation as long as an application for a wiretap order is made within 48 hours. A law enforcement officer, designated by the U. S. Attorney General, can initiate an emergency interception only when an organized crime conspiracy or threat to national security exists. Applications and orders for emergency wiretaps must satisfy the same requirements as for regular wiretaps.[31] According to the legislative history of the emergency wiretap provision, such a provision is necessary because it is often found that organized crime figures will call a meeting and

choose a meeting place simultaneously. To require a court order prior to initiation of the wiretap would be tantamount to failing to authorize the surveillance.[32]

EXECUTION

Title III also requires that the order specify that the wiretap must be executed as soon as practicable and in a way which minimizes the interception of communications not described in the application and order.[33] Minimization is usually accomplished by not intercepting conversations that are unlikely to contain incriminating statements. Thus, if a babysitter at the house where the interception is being conducted calls her boyfriend, the call probably should not be monitored. In practice, it has proven difficult to minimize interception of non-incriminating private conversations. Because the contents of conversations cannot be predicted in advance, the overhearing of partial or complete conversations which are not authorized occur in almost every wiretap. In determining whether law enforcement officers have minimized the interception of irrelevant conversations, courts have generally resorted to a test of reasonableness based on the circumstances known to the officers at the time of interception. Thus, even if intercepted conversations later prove to be pertinent, they may not be used to obtain evidence or as evidence in a criminal trial if at the time they were intercepted the circumstances did not warrant such interception.[34] Minimization is intended to prevent violations of the

Constitution's Fourth Amendment prohibition against general searches.

An order authorizing an interception may also require periodic reports to the issuing judge showing the progress being made on the interception.[35] Title III also sets out safeguards to insure that accurate records are kept of intercepted communications. The law requires that the communication be recorded if possible. Immediately upon the termination of an interception, the recordings must be given to the issuing judge and sealed along with the application(s) and order(s). Applications, orders, and recordings may be destroyed after 10 years, by order of the judge.[36]

Notice of the wiretap must be given to the person named in a wiretap order within 90 days after the termination of the interception or the denial of a wiretap application. A judge may also order notice to other persons whose conversations are intercepted. The notice must include whether the application was granted, the period of interception, and whether any communications were intercepted. The judge may order disclosure of the contents of the communications intercepted, the applications, and the orders to persons whose conversations are intercepted.[37] However, if evidence obtained as a result of wiretapping is to be used in a trial, the applications and wiretap orders must be disclosed to the defendant 10 days before the trial.[38]

USE OF WIRETAP EVIDENCE

The purpose of wiretapping is, of course, to obtain evidence to prosecute criminals. Title III also sets out procedures and standards for the use of evidence obtained as a result of wiretapping.

Any evidence obtained as a result of a legally authorized interception may be disclosed by one law enforcement officer to another so long as it is appropriate to the proper performance of either person's official duties.[39] This provision is designed to encourage information sharing within the law enforcement community and to encourage Federal, state and local cooperation.[40] A law enforcement officer may also use legally obtained wiretap evidence in the performance of his official duties, such as establishing probable cause for search or arrest, or developing witnesses.[41]

Legally obtained wiretap evidence can also be used as evidence in any criminal case or grand jury proceeding.[42] Such evidence can be used at trial to establish guilt directly, or to corroborate, impeach, or refresh the recollection of witnesses.[43] If information or evidence of crimes other than those specified in an interception order are obtained, it can be used by law enforcement officers in the proper performance of their official duties. For use by any person in a criminal proceeding, a judge must find in a subsequent application that the interception was proper.[44] The application would need to include a

showing that the original order was lawfully obtained, that it was sought in good faith and not as a "subterfuge" search, and that the communication was incidentally intercepted during the course of a legally executed wiretap.[45]

EXCLUSION OF EVIDENCE

Evidence obtained through or as a result of an illegal wiretap is not admissible in criminal proceedings against the person wiretapped. If such wiretap evidence is sought to be admitted against a party to an intercepted communication in a criminal case, that party can move to suppress the evidence. If the court decides that the communication was unlawfully intercepted; that the order of authorization was insufficient on its face; or that the interception was not made in conformity with the order of authorization, then any evidence obtained as a result of the wiretap will be suppressed or excluded from the trial.[46]

Whether all of the wiretap evidence or just parts of it are suppressed depends upon which particular provision of the statute is involved. If the court order itself is determined to have been invalid, then all the evidence obtained should be suppressed. However, where a wiretap is continued beyond the authorized period, or when there is no minimization, only that part of the wiretap evidence obtained after the authorization ended or during the period when

interception should not have occurred, may be suppressed.[47]

III. FEDERAL REGULATION OF COURT-ORDERED WIRETAPPING BY STATE OFFICIALS

The Federal wiretapping statute not only includes the requirements of the Federal Constitution with which state statutes must comply, but may also set forth additional Federal statutory standards with which state statutes must comply.

PREEMPTION

The power to regulate wiretapping may belong exclusively to the Federal government, except to the extent that the Federal government allows state regulation of wiretapping which does not conflict with Federal regulations. Generally, the powers of government in the United States are divided between the Federal and state governments by the United States Constitution. The Constitution itself grants specific powers to the Federal government and in particular to the Congress. All powers not granted to the Federal government are powers of the states.[48] If the Constitution grants to Congress the power to regulate an area, the Congressional legislation is supreme over any conflicting state legislation. Thus, Federal legislation may preempt inconsistent state legislation.

The U. S. Constitution grants to Congress the power to prohibit

unreasonable searches and seizures by state officials and to regulate interstate commerce.[49] It is now clear that wiretapping, including bugging, is a search and seizure under the Fourth Amendment. Thus, Congress has the power to enact legislation to prohibit unreasonable wiretapping by state officials. The Constitution also grants to Congress the power to regulate interstate commerce.[50] The Federal government using this power may regulate matters which occur totally within one state if there is an effect on interstate commerce. Thus Congress may regulate interception of communications by telephone and telegraph by state officials or private persons because interstate calls as well as intrastate (purely within a state) calls are made on the same facilities. Also, devices used in wiretapping including bugging may be manufactured or sold in interstate commerce. In addition, bugging may have an effect on interstate commerce because of the context of the bugging. For example, bugging a meeting of a business with offices in several states could affect interstate commerce. Because the U. S. Constitution has granted Congress the exclusive power to regulate interstate commerce, the states do not have power to regulate interstate commerce and state laws which interfere with Federal regulations or place an unreasonable burden on interstate commerce are unconstitutional.[51] This is called Federal preemption, since the Federal regulation preempts or prevents the states from regulating the same area in a conflicting manner. However, the Congress may allow states to regulate areas which affect interstate commerce.

Whether and to what extent states are preempted from regulating a specific area is a question of what Congress intended in enacting particular Federal legislation. It is clear that Congress intended to allow state regulation of wiretapping since the Federal statute expressly says so.[52] But there remains the question of whether and to what extent state statutes may differ from the Federal statute. The intent of Congress in passing the Federal wiretap statute was to set forth the minimum standards for protection of privacy which states must follow.[53] It is clear that Congress intended to allow the states to adopt stricter standards for the protection of privacy and to interpret their statutes more strictly than the Federal courts.[54]

Thus, it is generally felt that state statutes need not be identical with the Federal statute but must be in substantial conformity with it or establish stricter standards for the issuance of wiretap orders.[55] In particular, state statutes must be in substantial conformity with or stricter than the Federal statute as to the offense for which wiretap orders may be issued, who may apply for orders, who may issue orders and the standards for application, issuance and execution of orders.[56] However, it may be that a state statute is not required to list offenses, but that the offenses specifically listed in the Federal statute are then implied into the state statute.[57] There is a possibility that a state statute could satisfy both the U. S. Constitution and the Federal statute without specifying standards for the application for or issuance of wiretap orders, as long as

the state courts require standards as strict as the Federal statute before orders are issued.[58] However, it is generally believed that state wiretap statutes may differ from the Federal statute as to criminal liability and civil remedies.[59]

OFFENSES FOR STATE WIRETAPS

Generally, Title III allows states to enact statutes authorizing court-ordered wiretapping in the investigation of serious offenses. Title III specifies the crimes for which states may authorize wiretapping. These crimes are "murder, kidnapping, gambling, robbery, bribery, extortion, dealing in narcotic drugs, marihuana or other dangerous drugs, or other crimes dangerous to life, limb, or property, and punishable by imprisonment for more than one year, or any conspiracy to commit any of these offenses."[60] Because Congress intended to allow states to enact stricter standards for the protection of privacy, states may authorize wiretapping for any number of the allowable offenses or none at all.

WHO MAY APPLY

Title III provides that, if a state statute so allows, the principal prosecuting attorney of a state, or of any political subdivision of the state, can apply for a wiretapping order.[61] The principal prosecuting attorney of a state is usually the attorney

general. The principal prosecuting attorney of a political subdivision of a state would usually be a district attorney or a county prosecuting attorney.[62] In Hawaii, it is most probable that the Attorney General and the county prosecuting attorneys can be empowered to apply for wiretap orders.

WHO MAY ISSUE

The Federal law allows states to authorize any judge of a court of general criminal jurisdiction to issue wiretap orders.[63] General criminal jurisdiction probably means jurisdiction over most criminal offenses and proceedings. In Hawaii, the district courts do not have jurisdiction over all crimes, nor over felony trials (most offenses for which wiretaps may be employed are felonies). Thus, the Federal statute may prevent Hawaii from giving district court judges the authority to issue wiretap orders, unless general criminal jurisdiction includes misdemeanor jurisdiction and/or jurisdiction over some felony proceedings other than trial. Hawaii circuit courts are probably courts of general criminal jurisdiction since they have jurisdiction over all criminal trials by jury. Additionally, Hawaii's Supreme Court probably could be empowered to issue wiretap orders. Although the Hawaii Supreme Court has appellate jurisdiction, its jurisdiction includes all offenses. The U. S. Court of Appeals, also appellate courts, are allowed to issue wiretap orders.[64]

STATE WIRETAP ORDERS

State applications and orders for wiretaps must satisfy the same statutory requirements as Federal applications and orders, as described previously.

IV. PROHIBITING UNAUTHORIZED WIRETAPPING

In order to protect privacy by enforcing the standards and procedures for court-ordered wiretapping, the Federal statute provides both criminal penalties and civil liability for wiretapping which violates those standards.

CRIMINAL PENALTIES

The law makes criminal the willful interception, disclosure, and use of communications where the interception is in violation of the statute.[65] Because the scope of the statute is limited, as previously discussed, there is no criminal liability for consensual interception, interceptions by use of an extension telephone or party lines, nor for business interception by communications carriers and the Federal Communications Commission. Additionally, the manufacture, distribution, possession, or advertising of a wiretapping device is made criminal[66] and these devices can be confiscated.[67] A good faith reliance upon a court order is a complete defense to criminal

charges,[68] even though the court order is invalid and the interception is thus unauthorized. The maximum penalty for any violation is five years imprisonment and a $10,000 fine.[69]

CIVIL LIABILITY

Title III also provides civil liability for unauthorized wiretapping in order to deter illegal wiretapping and compensate persons who suffer damages as a result of illegal wiretapping. Any person whose wire or oral communication is intercepted, disclosed, or used in violation of Title III has a civil cause of action against any person who intercepts, discloses or uses such communication or procures any person to do the same. The Federal statute provides for recovery of (1) actual damages, with a minimum recovery of $100 per day, or $1,000, whichever is greater; (2) punitive damages, where malice is shown; and (3) reasonable attorney's fees and other litigation costs. Actual damages include economic, physical, and intangible, psychological injuries such as invasion of privacy, anxiety, lowering one's reputation in the community, etc. The Federal statute provides for minimum damages in order to encourage suit which can be costly and uneconomic where damage awards are small. Minimum damages of $1,000 also recognize that any invasion of privacy is a serious and substantial injury, although difficult to assess in terms of a dollar and cents figure. As in criminal liability, a good faith reliance on a court order is a complete defense to an action for damages even

though the order may be illegal.

V. CONCLUSION

Thus, the Federal wiretapping statute provides detailed procedures and standards for Federal and state court-ordered wiretapping and attempts to prohibit other unauthorized wiretapping by criminal penalties, civil liability and exclusion of evidence in criminal cases. In this way, the Federal statute attempts to accomplish the somewhat inconsistent purposes of fighting organized crime while protecting individual privacy.

Because of Federal preemption in regulating wiretapping, states probably must enact statutes which require (1) a sworn, written application; (2) including a statement of the authority for the application; (3) the identity of the applicant and authorizing person; (4) a statement of circumstances as to why there should be a wiretap including; (5) details of the offenses involved; (6) details of the place of the interception and facilities to be used; (7) a description of the type of communications to be intercepted; (8) the identity of the person committing the offense involved; (9) details of the failure or dangerousness of other means of investigation; (10) the proposed duration of the wiretap and why it should last that long; and (11) details of previous applications involving the person or facilities involved. Any state statute must also specify that there must be

(1) probable cause that the person named in the order or using the facilities to be wiretapped will commit, is committing or has committed the offense specified in the application; (2) probable cause that incriminating statements concerning the offense will be made through the facilities being wiretapped; and (3) that other investigations have failed, will probably fail, or are too dangerous.

State statutes probably must also not specify offenses which are not included in the Federal statute, may not allow applications for wiretaps unless authorized by the chief prosecuting official of the state or political subdivision of the state, and may not allow anyone other than judges of courts of general criminal jurisdiction to issue wiretap orders. As long as a state statute does not do these things, the state should be free to depart from the language, format, procedures and substance of the Federal wiretapping statute, especially in the areas of criminal and civil liability.

FOOTNOTES

CHAPTER III - THE FEDERAL WIRETAP STATUTE

[1] 18 United States Code ("U.S.C.") §2510-20 (1970).

[2] 1968 U.S. Code Cong. & Ad. News 2157 (S. Rep. No. 1097, 90th Cong., 2d Sess., 1968).

[3] Ibid., p. 2153.

[4] Ibid., P. 2153.

[5] 18 U.S.C. §2516(1) (1970).

[6] 18 Ibid., §2511.

[7] 18 Ibid., §2516(2).

[8] 18 Ibid., §2510(1).

[9] 1968 Code Cong. & Ad. News at note 2, pp. 2177-78.

[10] 18 U.S.C. §2510(2) (1970).

[11] Ibid., §2511(c)-(d).

[12] Ibid., §2511(2)(a).

[13] Ibid., §2511(2)(b).

[14] Ibid., §2511(3).

[15] Ibid., §2511(3).

[16] 1968 U.S. Code Cong, & Ad. News at note 2, p. 2186. *Other offenses were included because they relate to national security.*

[17] 18 U.S.C. §2516(1) (1970).

[18] Ibid., §2510(7).

[19] Ibid., §2516(1).

[20] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2185.

[21] 18 U.S.C. §§2510(9), 2518(1) (1970).

[22] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2185.

[23] 18 U.S.C. §2518(1)(a)-(e) (1970).

[24] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2190.

[25] 18 U.S.C. §2518(1)(f) (1970).

[26] Ibid., §2518(3).

[27] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2191.

[28] 18 U.S.C. §2518(4)(a)-(e) (1970).

[29] Ibid., §2518(5).

[30] Ibid., §2518(5).

[31] Ibid., §2518(7).

[32] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2193.

[33] 18 U.S.C. §2518(5) (1970).

[34] Carr, Electronic Surveillance, pp. 255-267 (1977).

[35] 18 U.S.C. §2518(6) (1970).

[36] Ibid., §2518(8)(a)-(b).

[37] Ibid., §2518(8)(d).

[38] Ibid., §2518(9).

[39] Ibid., §2517(1).

[40] 1968 Code Cong. & Ad. News at note 2, p. 2188.

[41] 18 U.S.C. §2517(2) (1970); 1968 U.S. Code Cong. & Ad. News at note 2, p. 2188.

[42] 18 U.S.C. §2517(3) (1970).

[43] 1968 U.S. Code Cong. & Ad. News at note 2, pp. 2188-89.

[44] 18 U.S.C. §2517(5) (1970).

[45] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2189.

[46] 18 U.S.C. §2518(10)(a) (1970).

[47] Carr, op. cit., p. 279.

[48] Tenth Amendment, U. S. Constitution.

[49] Fourteenth Amendment, Sec. 5, U. S. Constitution.

[50] Art. 2, Sec. 8, U. S. Constitution.

[51] See, e.g., Rice v. Santa Fe Elevator Corp., 331 U.S. 218 (1947).

[52] 18 U.S.C. §2516(2) (1970).

[53] Carr, op. cit., §2.04[1], p. 29.

[54] Ibid.

[55] Ibid., §2.04[2].

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] 18 U.S.C. §2516(2) (1970).

[61] Ibid., §2516(2).

[62] 1968 U.S. Code Cong. & Ad. News at note 2, p. 2187.

[63] 18 U.S.C. §§2510(9), 2516(2) (1970).

[64] Ibid., §2510(9).

[65] Ibid., §2511(1).

[66] Ibid., §2512(1).

[67] Ibid., §2513.

[68] Ibid., §2520.

[69] Ibid., §2511(1).

CHAPTER IV

SURVEY OF STATE WIRETAP STATUTES

I. INTRODUCTION

Twenty-three states and the District of Columbia have enacted statutes which allow court-ordered wiretapping in criminal investigations.[1] The general purpose of state wiretap statutes is the same as that of the Federal statute: to combat organized crime while protecting privacy. The state statutes attempt to accomplish this purpose by setting strict standards for court-ordered wiretapping and prohibiting other unauthorized wiretapping. Most state statutes are modeled after, and are almost identical to, the Federal statute because the Federal statute is thought to be preemptive.[2]

While most states have adopted both the format and substance of the Federal statute, several states have enacted legislation which places stricter limitations on court-ordered wiretapping.[3] Other differences in the Federal and state statutes reflect local differences in the structure of state judiciaries and the needs of local law enforcement. The following chapter attempts to highlight the varying substantive provisions of state statutes.

II. SCOPE OF STATE STATUTES

The scope of state statutes is identical to that of the Federal statute except that state statutes do not apply to Federal officials acting in the course of their employment. State statutes, like the Federal statute, recognize exceptions for consensual wiretapping, wiretapping by use of an extension phone or party line, and necessary exceptions for certain businesses and agencies such as telephone companies and the Federal Communications Commission.

Although almost all states allow wiretapping with the consent of a party to a conversation, eleven states require the consent of all parties for consensual wiretapping.[4] However, of these, California, Georgia, Massachusetts, Michigan, Montana and Oregon allow one-party consent monitoring by law enforcement officers without a court order in the interest of preventing or detecting a crime.* Oregon makes a distinction between the interception of wire communications for which the consent of one party is sufficient, and the interception of other types of communications which requires the consent of all parties involved.

Montana and Oregon allow one-party consensual monitoring by any public official in the performance of his or her duties.

III. COURT-ORDERED WIRETAPPING

All state wiretap statutes allow certain state law enforcement officers to wiretap pursuant to a court order.

OFFENSES

Most state statutes authorize court-ordered wiretaps only for specific offenses. Designated offenses can be as encompassing as those in New York's statute which lists all types of offenses and their degree of severity, or as limiting as that of Pennsylvania which authorizes court-ordered wiretaps only when a police officer's life is endangered. Commonly designated offenses that are included in most state statutes are: murder, robbery, kidnapping, extortion, bribery, drug abuse, and gambling. Other less commonly designated offenses are: prostitution, obstruction of justice, dealing in stolen goods, auto theft, embezzlement, usury, arson, and riot. Other states allow wiretapping for any felony dangerous to life, or to life, limb and property.[5]

WHO MAY APPLY

In most states, the attorney general, the prosecuting attorney, the county attorney, or their designates are authorized to apply for a wiretap order. Some states allow applications only by the attorney

general, or by his designate in the attorney general's absence.[6] Florida also allows its Governor and Department of Criminal Law Enforcement to apply for court-ordered wiretaps. New Jersey's State Commission on Investigation is also given such authorization. Wisconsin requires the Attorney General and District Attorney to apply jointly.

WHO MAY ISSUE ORDERS

Most state statutes authorize any judge of a state court having jurisdiction over felony criminal trials to authorize a wiretap. Several statutes also authorize a judge of a state appellate court to authorize wiretaps.[7] Some state statutes are more specific, however. Connecticut requires the unanimous approval of wiretap applications by a designated three-judge panel. New Jersey and Delaware call for the Chief Justice of that state to periodically designate a judge to review applications. The Wisconsin statute specifies that in those counties having more than one branch of the circuit court, applications must go to the circuit court judge of the lowest branch having criminal jurisdiction. The purpose of specifying a certain judge or court to hear applications is to prevent "forum shopping", the practice of choosing the most sympathetic judge.

WIRETAP ORDERS

The state statutes without exception follow the requirements and

procedures in the Federal statute regarding wiretap applications and orders, as set out in Chapter III.[8] Some states require that necessary cooperation by communications carriers in conducting the wiretap be specified in the court order.[9] Massachusetts and New York require that the court order specify if entry into any building is necessary to install wiretapping devices.

EMERGENCY WIRETAPS

Only Delaware, the District of Columbia, Nevada, and New Jersey allow emergency wiretaps without a court order. The procedures under these state statutes are identical to the provision of the Federal statute.

DURATION

Most states allow a 30-day period of surveillance for an original wiretap order and unlimited numbers of court-ordered extensions of 30-day periods, as provided in the Federal statute. However, eight states provide for shorter periods of 10, 15, or 20 days.[10] Most states place a limit on the number of extensions that may be authorized.[11] For example, New Jersey allows only two 10-day extensions; Connecticut restricts the total number of wiretaps allowed per year to 34 orders and allows three 10-day extensions of each wiretap; while Colorado, Georgia and Washington authorize only one extension of the original

order. Other states allow an unlimited number of extensions like the Federal statute.[12] However, all state statutes provide that a wiretap shall automatically terminate upon attainment of its objective, as both the U. S. Constitution and the Federal statute require.

EXECUTION

The state statutes are identical to the Federal statute in requiring that every court order shall include a directive to initiate the wiretap as quickly as possible and to minimize the resulting invasion of privacy. New Jersey and Massachusetts attempt to achieve minimization by limiting the hours and days of interception. Additionally, many statutes specify that privileged communications cannot be intercepted or used as evidence.[13] Privileged communications are confidential communications between a person and his doctor, lawyer, clergyman, or spouse.[14] However, Delaware and New Jersey allow the wiretap of a privileged conversation upon a showing of "special need." Pennsylvania's statute, one of the most restrictive, forbids the recording of any wiretapped conversation.

NOTICE/DISCLOSURE

Notice of a wiretap is generally required to be served on a person named in the application after the termination of the wiretap. A judge may also require notice to any other party whose communication

is intercepted by the wiretap. Most state statutes follow the Federal statute and require that this notice be served within 90 days after the filing of an application which is denied or after the termination of the wiretap. In addition, the majority of states require notice of the existence of the wiretap to be served 10 days before any court proceeding concerning the admissibility of evidence obtained by wiretap. Georgia provides that notice shall be given upon indictment of a person who has been wiretapped. Massachusetts provides that notice must be served within 30 days of the termination of the wiretap, unless postponed by the judge, but in no event later than three years after the wiretap is ended. As in the Federal statute, most state statutes allow the issuing judge to decide whether to disclose the contents of the intercepted conversations to any persons who were wiretapped. In Georgia and Massachusetts, disclosure of the contents to a party to the intercepted conversations is mandatory.

CUSTODY OF INTERCEPTED COMMUNICATIONS

Most states have procedures similar to those of the Federal statute, which provide for the safeguarding and prompt return to the court of wiretap evidence. Many states require the storage of wiretap records for up to five years and some up to 10 years. Georgia requires that all wiretap evidence be destroyed immediately if no incriminating communications were obtained.

INTERLOCUTORY APPEAL

Twelve state statutes allow an immediate appeal from a judge's decision to exclude wiretap evidence from a criminal trial. Usually appeals are not allowed until the criminal case is completed. If an immediate appeal is not allowed, the prosecution may lose the case without the wiretap evidence and be unable to prosecute the same case again, even if a later appeal is successful. Rhode Island and some other states also allow an appeal from a denial of a wiretap application.

REPORTS

Many states require annual reports of wiretap activities to be filed either with the state's Chief Justice, judicial council, committee, or legislature. The Federal wiretapping law also requires all state judges and law enforcement officials to report annually concerning applications for wiretap orders.

IV. PROHIBITING UNAUTHORIZED WIRETAPS

The state statutes, like the Federal, enforce the prohibition against unauthorized wiretapping by providing criminal penalties and civil liability, and by prohibiting the use of evidence obtained as a result of unauthorized wiretaps.

CRIMINAL PENALTIES

All state wiretapping statutes follow the Federal model in prohibiting the unauthorized interception, use, or disclosure of any wire or oral communication. Almost all state statutes also prohibit the manufacture, marketing or possession of devices designed primarily to intercept private communications.[16] Generally, statutes outlawing wiretapping devices also allow the confiscation of such equipment. In addition, Arizona and New York require a telephone company to inform law enforcement officers of any wiretap violation coming within its knowledge.

Criminal penalties for wiretapping violations range from a $500 maximum fine in Alabama to a maximum of seven years in prison in Delaware and six years in Nevada. Many other state statutes provide the same maximum penalty as the Federal statute: five years in prison and a $10,000 fine;[17] most of the remaining state statutes make wiretapping offenses misdemeanors, a less serious crime, with a maximum penalty of less than a year in prison and a fine of $1,000 or less.[18] Some states provide different penalties for different types of wiretapping violations, depending upon the seriousness of the offense. California, for example, provides different penalties for disclosure and possession of wiretap devices and allows a more severe penalty for the second violation.

EXCLUSION OF EVIDENCE

More than half of the state statutes expressly provide that evidence obtained in an illegal wiretap or as a result of an illegal wiretap cannot be used as evidence at the criminal trial of a party to the conversation.[19] Since it is generally accepted that evidence obtained as a result of illegal action by state officials cannot be used in a criminal trial against the person wronged, it is probable that all states prohibiting unauthorized wiretapping would not allow use of the evidence in a criminal trial against a person who was wiretapped.

CIVIL ACTION FOR DAMAGES

Sixteen state statutes, like the Federal statute, expressly allow a party whose conversations are illegally intercepted a civil action for damages.[20] All statutes allow the person whose privacy was invaded to recover actual damages incurred as a result of the illegal wiretap. Thirteen of these states have followed the Federal statute and allow recovery of actual damages with minimum damages of $100 for each day of wiretapping with a $1,000 minimum recovery, in addition to punitive damages and costs of suit.[21] Pennsylvania provides only a $100 minimum recovery. Minnesota awards three times the actual damages (known as treble damages) with a minimum of $1,000. In addition to damages, Minnesota specifically provides for injunctive relief, a

court order directing certain persons to cease the unauthorized wiretapping. Most state statutes make good faith reliance on a court order as a complete defense against any civil or criminal action brought under the wiretap statute.[22] However, Nebraska's statute does not include the good faith defense.

V. CONCLUSION

While most states have adopted wiretap statutes substantially identical to the Federal wiretap statute, it is apparent that many states attempt to further protect privacy by the use of additional controls on court-ordered wiretapping.

Many states have attempted to further protect privacy by limiting such things as: (1) the offenses for which wiretaps can be ordered; (2) who may apply for wiretap orders; (3) who may issue wiretap orders; (4) the factual situation in which orders may be issued; (5) the duration of wiretaps; and (6) by providing other procedures for judicial control of the use of wiretaps.

COMPARISON OF WIRETAP STATUTES

	ARIZONA	COLORADO	CONNECTICUT	WASHINGTON, D.C.	DELAWARE	FLORIDA	GEORGIA	KANSAS	LOUISIANA
1. EXCEPTION WITH CONSENT (CONSENT OF 1 REQUIRED UNLESS NOTED OTHERWISE	x	x	x	x	Consent of all parties required except for police, then consent of 1 party	x	Consant of all parties required	***	
2. OFFENSES	Felony dangerous to life, limb, or property; conspiracy; B,K,M,G,BRI,N,R	Felony; conspiracy; BUR,G,K,M,R,BRI,N, E,T,ASS,RA,Misuse of official info	Felonious crimes of violence; G	ARS,BLK,BRI,BUR,D, G,L,K,M,N,R; Obstruction of Justice Receiving Stolen Goods	Felony; conspiracy; M,K,G,R,BRI,E,N	Conspiracy;M,K,G, R,BUR,L,PR,U,BRI, ABORT,E,N	State or national recurity; Felony involving bodily harm: K,N,BUR,P,T,BLK,G, ALC,AUTO,BRI	Directly relating to safety of human life or national security; Conspiracy;M,K,BRI, R,T; Racketeering; Tampering with sports contests	
3. APPLICANT(S)	County Attorney or Attorney General	Attorney General or District Attorney	State's Attorney for County	U.S. Attorney	Attorney General	Governor; Dept. of Criminal Law Enforcement; State or County Attorney	Attorney General or District Attorney	Attorney General; District Attorney; or County Attorney	
4. AUTHORIZING JUDGE(S)	Supreme Court Justice; Judge of Ct. App.;** Superior Court Judge	Judge of Supreme or District Court	Panel of 3 Superior Court Judges designated by Chief Justice	U.S.D.C.,** Ct. App., court of general criminal jurisdiction	Designated Superior Court Judge	Supreme Court; Ct. App., Superior Ct. having criminal jurisdiction	Superior Court Judge	Supreme Court or District Court	
5. MAXIMUM DURATION OF WIRETAP	30 days	30 days	10 days	30 days	30 days	30 days	20 days	30 days	
6. EXTENSION (DURATION AND NUMBER ALLOWED)	1 extension 30 days	1 extension 30 days	3 extensions 10 days	1 extension 30 days	1 extension 30 days	1 extension 30 days	1 extension 20 days	1 extension 30 days	
7. EMERGENCY WIRETAPS	***			X	X				
8. CRIMINAL PENALTIES FOR ILLEGAL INTERCEPTION, USE, OR DISCLOSURE	2 years/$1,000; Duty to report violation $500	Class 5 felony	Class D felony	For possession of device also 5 years/$10,000	For possession of device also 7 years	For possession of device also 3rd degree felony	5 years/$10,000	1 year/$500	3 months/$300
9. CIVIL ACTION			X	X	X	X		X	
10. DAMAGES			$100/day $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum		$100/day $1,000 minimum	
11. UNUSUAL FEATURES			Exception for confidential relationship; Suppress on grounds of improper sealing of tapes	Emergency procedure only for organized crime activity					

**Ct.App. - Court of Appeals
U.S.D.C. - U.S.District Court

***Empty box indicates that statute is silent as to issue.

ABBREVIATIONS OF OFFENSES

ABORT-*Abortion*
ALC -*Alcoholic Beverage Law*
ARS -*Arson*
ASS -*Assassination*
AUTO-*Auto Theft*
BLK -*Blackmail*
BRI-*Bribery*
BUR-*Burglary*
D-*Drug Offenses*
E -*Extortion*
EM-*Embezzlement*
F -*Forgery*
G-*Gambling*
K-*Kidnapping*
L-*Larceny*
M-*Murder*
N-*Narcotics*
P-*Perjury*
PR-*Prostitution*
R-*Riot*
RA-*Rape*
T-*Theft*
U-*Usury*

	MARYLAND	MASSACHUSETTS	NEBRASKA	MINNESOTA	NEW HAMPSHIRE	NEVADA	NEW JERSEY	NEW MEXICO	NEW YORK
1. EXCEPTION WITH CONSENT (CONSENT OF 1 REQUIRED UNLESS NOTED OTHERWISE)	x		x	x	Consent of all parties required	x	x		
2. OFFENSES		Conspiracy in connection w/organized crime;ARS,ASS,E,BRI, BUR,EM,F,G,K,L,U,M, N,P,PR,R;Battery; Intimidating Juror; Mayhem	Conspiracy; M,K, BRI,E,N,G,	Felony;conspiracy; M,ASS,R,K,RA,PR, BRI,P,F,	Organized crime; conspiracy; M,K, G,BRI,E,BLK,N	Any offense made felony under Ch. 453 or 454;M,K,R,E,BRI; Destruction of public property by explosives	Conspiracy;aiding criminals;M,G,R,BRI, E,N,ARS,BUR,EM,F,L; Escape;Loansharking; Receiving stolen property	Organized criminal conspiracy;certain offenses punishable by more than 1 year jail:M,K,E,R,N,BUR, RA,ARS,Mayhem	Conspiracy; See Statute§ 700.05(8)
3. APPLICANT(S)	State's Attorney of the County or of Baltimore	Attorney General, District Attorney or their deputies	Attorney General or County Attorney	Attorney General or Designated Assistant or County Attorney	Attorney General; Deputy Attorney General;County Attorney	Attorney General or District Attorney	Attorney General, County Prosecutor or State Commission of Investigation	Attorney General or District Attorney	Attorney General, District Attorney or their designate
4. AUTHORIZING JUDGE(S)	Circuit Court of County or Supreme Bench of Baltimore	Superior Court Justice	District Court Judge	Supreme Court or District Court Judge	Superior Court Judge	Supreme Court Justice or District Judge	Superior Court Judge as designated by Supreme Court Judge	District Court Judge	App. Court Justice Sup. Court Justice or County Court Judge
5. MAXIMUM DURATION OF WIRETAP	30 days	15 days	30 days	10 days	10 days	30 days	20 days	30 days	30 days
6. EXTENSION (DURATION AND NUMBER ALLOWED)		1 extension 15 days	1 extension 30 days	1 extension 10 days	1 extension 10 days	1 extension 30 days	2 extensions 10 days	1 extension 30 days	1 extension 30 days
7. EMERGENCY WIRETAPS		--			x		x	--	
8. CRIMINAL PENALTIES FOR ILLEGAL, INTERCEPTION, USE, OR DISCLOSURE	1 year/$500	For possession of device also 2 years/$5,000	3 years/$500 minimum-1 year/$500	For possession of device also 5 years/$10,000	For possession of device also 5 years/$10,000	6 years/$5,000 Minimum-1 year	For possession of device also 5 years/$10,000	Misdemeanor	Class E felony:possession of device -Class A misdemeanor;Failure to report-Class B misdemeanor;Disclosure-Class A misdemeanor
9. CIVIL ACTION		x		Injunctive Relief x	x	x	x	x	
10. DAMAGES		$100/day $1,000 minimum		Treble damages $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum	
11. UNUSUAL FEATURES	Registration of device required	Party is notified before wiretap; D. has copy of wiretap by right	If court order is illegal, there is a violation				Additional grounds required to wiretap privileged communications		

	OREGON	PENNSYLVANIA	RHODE ISLAND	SOUTH DAKOTA	VIRGINIA	WASHINGTON	WISCONSIN	FEDERAL STATUTE	HAWAII HB-412
1. EXCEPTION WITH CONSENT (CONSENT OF 1 REQUIRED UNLESS NOTED OTHERWISE)		Consent of all parties required			X	Consent of all parties required	X	X	X
2. OFFENSES	Directly and immediately affecting safety of human life or national security	When life of police officer is in jeopardy	Violation of Ch. 19 & 47 of Title II, where imprisonment is more than 1 year M,R,K,E,L,U,N	Conspiracy; M,K,G,R, BRI, E, N, RA	Felonious offense; E,BRI	Conspiracy;national security;endangerment of human life; R,ARS	Conspiracy; M,K, G,BRI,E,N	BRI,E,K,ASS,M,N,R; Conspiracy;treason; espionage; sabotage; robbery; etc.	M,K,G,Robbery,BRI, E,N,Marijuana or other dangerous drugs,any other crime dangerous to life,limb or property & punishable by imprisonment for more than 1 yr.
3. APPLICANT(S)	District Attorney	Attorney General, District Attorney, or their designate	Attorney General or his designated assistant	Attorney General, State's Attorney	Attorney General or Attorney for the Commonwealth	Attorney General or County Prosecuting Attorney	Attorney General together with District Attorney	U. S. Attorney General, Assistant Attorney General	Attorney General, County or Prosecuting Attorney, authorized representatives
4. AUTHORIZING JUDGE(S)	Circuit or District Judge	Judge of court of record having jurisdiction	Superior Court Justice	Circuit Court Judge	Judge of court of record having criminal jurisdiction	Superior Court Judge	Circuit Court Judge having criminal jurisdiction	U. S. Court of Appeals Judge; U.S. District Court Judge	Circuit Court Judge;District Court Judge
5. MAXIMUM DURATION OF WIRETAP	60 days	30 days	30 days		15 days	15 days	30 days	30 days	30 days
6. EXTENSION (DURATION AND NUMBER ALLOWED)	1 extension for 60 days; unlimited additional extensions of 30 days	Unlimited, 30 days	Unlimited, 30 days		Unlimited, 15 days	1 extension 15 days	Unlimited 30 days	Unlimited 30 days	Unlimited 30 days
7. EMERGENCY WIRETAPS								X	X
8. CRIMINAL PENALTIES FOR ILLEGAL, INTERCEPTION, USE, OR DISCLOSURE	3 years/$3,000 Disclosure-5 years/ $4,000	Second Degree Misdemeanor	5 years	Misdemeanor	For possession of device also 5 years/$1,000	Gross Misdemeanor	For possession of device also 5 years/$10,000	5 years/$10,000	5 years/$10,000
9. CIVIL ACTION		X	X		X	X	X	X	X
10. DAMAGES		$100 minimum	$100/day $1,000 minimum		$100/day $1,000 minimum		$100/ day $1,000 minimum	$100/day $1,000 minimum	$100/day $1,000 minimum
11. UNUSUAL FEATURES		Cannot record conversation; ct order required for 1 pty. consent			Notice may be postponed for 30-day periods;judge hearing application disqualified from hearing motion to suppress				

FOOTNOTES

CHAPTER IV - SURVEY OF STATE WIRETAP STATUTES

[1]Arizona, Colorado, Connecticut, Delaware, Florida, Georgia, Kansas, Maryland, Massachusetts, New Jersey, New Mexico, New York, Oregon, Pennsylvania, Rhode Island, South Dakota, Virginia, Washington and Wisconsin have statutes which allow court-ordered wiretapping. Ariz. Rev. Stat. §13-1051 et.seq. (1975 Supp.); Colo. Rev. Stat. §18-9-201 et.seq. (1973); Conn. Gen. Stat. §53a-187 et.seq. (1975 Supp.); Del. Code §1336 et.seq. (1974); Fla. Stat. Ann. §934.01 et.seq. (1975 Supp.); Ga. Code Ann. §26-3001 et.seq. (1972); Kan. Stat. §22-2514 et.seq. (1974); Md. Ct. & Jud. Proc. Ann. Code, C.J. §10-401 et.seq. (1974); Mass. Gen. Law Ann., Chap. 272, §99 (1974 Supp.); Minn. Stat. Ann. §626A.01 et.seq. (1975 Supp.); Neb. Rev. Stat. §86-701 et.seq. (1971); Nev. Rev. Stat. §179.410 et.seq. and §200.610 et.seq. (1973); N.H. Rev. Stat. Ann. §570-A:1 et.seq. (1974); N.J. Stat. Ann. §2A:156A-1 et.seq. (1971); N.M. Stat. §40A-12-1.1 et.seq. (1973 Supp.); N.Y. Crim. Proc. Law §700.05 et.seq. (1971 McKinney) and N.Y. Penal Law §250.00 et.seq. (1967 McKinney); Or. Rev. Stat. §141.720 et.seq. (1974); Pa. Stat. Ann. §5701 et.seq. (1967 Purdon); R.I. Gen. Laws §12-5.1-1 et.seq. (1974 Supp.); S.D. Comp. Laws §23-13A-1 et.seq. (1974 Supp.); Va. Code Ann. §19.1-89 et.seq. (1975 Supp.); Wash. Rev. Code Ann. §9.73.030 et.seq. (1974 Supp.); Wisc. Stat. Ann. §968.27-33 et.seq. (1975 Supp.). See also D.C. Code §23-541 et.seq. (1973).

[2]Ringel, Searches and Seizures Arrests and Confessions, §320, p. 407 (1972).

[3]*See, e.g. Connecticut, New Hampshire, Pennsylvania and Washington statutes cited in footnote 1 above.*

[4]California, Ann. Cal. Code Penal §630 et.seq. (1970); Delaware; Georgia; Kansas; Maine; Massachusetts; Michigan, Mich. Comp. Laws Ann. §750.539 et.seq. (1976); New Hampshire; New Mexico; Pennsylvania; and Washington. See footnote 1 for citations to state statutes above.

[5]*See Arizona, Connecticut, Georgia, Kansas, Minnesota, Nevada, Oregon, Rhode Island and Virginia statutes. Of these, Connecticut, Georgia, Kansas, Oregon, and Washington allow wiretapping only where there is danger of bodily harm.*

[6]*See Delaware, Rhode Island, and Wisconsin statutes.*

[7]*Arizona, Colorado, Connecticut, District of Columbia, Florida, Kansas, Maryland, Minnesota, Nevada, and New York.*

[8]See pp. 40-42 of Chapter III.

[9]See, e.g., Va. Code Ann. §19.1-89.8 (1975 Supp.).

[10]Conn. Gen. Stat. §54-41(f) (1975 Supp.) (10 days); Ga. Code Ann. §26-3004 (1972) (20 days); Mass. Gen. Laws Ann., Chap. 272 §99(I) (1974 Supp.) (15 days); Minn. Stat. Ann. §626A-06(5) (1975 Supp.) (10 days); N.H. Rev. Stat. Ann. §570-A:9(V) (1974) (10 days); N.J. Stat. Ann. §2A:156A-13(f) (1971) (20 days); Va. Code Ann. §19.1-89.8 (1975 Supp.) (15 days); Wash. Rev. Code Ann. §9.73.040(6) (1974 Supp.) (15 days).

[11]*Arizona (1 extension); Colorado (1); Connecticut (3); District of Columbia (1); Delaware (1); Florida (1); Georgia (1); Kansas (1); Massachusetts (1); Nebraska (1); New Hampshire (1); Nevada (1); New Jersey (2); New Mexico (1); New York (1); and Washington (1).*

[12]*Louisiana, Maryland, Oregon, Pennsylvania, Rhode Island, Virginia and Wisconsin.*

[13]*See, e.g., District of Columbia, Delaware, Florida, Georgia, New Jersey and Rhode Island statutes.*

[14]*See, e.g., District of Columbia and New Jersey statutes.*

[15]*Colorado, District of Columbia, Delaware, Florida, Kansas, Nebraska, Minnesota, New Hampshire, New Jersey, New Mexico, Pennsylvania and Wisconsin.*

[16]*Rhode Island and South Dakota's statutes do not prohibit the possession, etc. of wiretapping or bugging devices.*

[17]*California, District of Columbia, Georgia, Maine, New Hampshire, New Jersey and Wisconsin.*

[18]*See, e.g., Kansas, Louisiana, Maryland, New York, Pennsylvania and Washington statutes.*

[19]*Colorado, Connecticut, Delaware, Florida, Kansas, Massachusetts, Minnesota, Nebraska, New Hampshire, New Jersey, New Mexico, New York, Pennsylvania, South Dakota, Virginia and Wisconsin.*

[20]*Connecticut, District of Columbia, Delaware, Florida, Kansas, Massachusetts, Minnesota, New Hampshire, Nevada, New Jersey, New Mexico, Pennsylvania, Rhode Island, Virginia, Washington and Wisconsin.*

[21] *Pennsylvania, Minnesota and Washington do not follow the Federal damages provision.*

[22] *Arizona, Colorado, Connecticut, District of Columbia, Delaware, Florida, Georgia, Kansas, Massachusetts, Minnesota, New Hampshire, New Jersey, New Mexico, Nevada, Rhode Island, Virginia, and Wisconsin.*

CHAPTER V

EFFECTIVENESS OF WIRETAPPING

I. INTRODUCTION

The problem in evaluating the effectiveness of wiretapping is the frequency and importance of the exceptions to the rule. To be sure, there are certain general conclusions that can be extracted from the mass of data collected by the Federal government on wiretapping activities throughout the nation, but the nature of such data is that the distinct features of individual cases are reflected, if at all, quite poorly. It is difficult to know, for example, whether wiretapping led to the successful investigation of a particularly heinous crime, or even whether it was an indispensable tool in the investigation of any crime, unless the circumstances surrounding the case are known. This means examining the pertinent court records, and assessing what may be called the quality of individual cases. Even after examining such records, there remains the additional difficulty of weighing the significance of these qualitatively-worthy, exceptional cases in comparison to the significance and the applicability of the general conclusions themselves.

II. GENERAL CONCLUSIONS

The general conclusions about wiretapping that can be made on the basis of the data provided by Federal and state agencies are as follows:

1. Wiretapping is useful in the investigation of gambling and narcotics but is seldom used against other crimes.

During the last four years, 1973 through 1976, more than 80% of all court-authorized wiretaps have been used in the investigation of gambling and narcotic cases. Other categories of crimes each account for, at the most, less than 5% of the total. In some years, wiretapping has been occasionally useful in loan sharking, usury and extortion cases; in other years, it was bribery or the fencing of stolen goods. Hardly ever was wiretapping used in homicide, burglary, kidnapping or arson investigations.[1]

Gambling and narcotics are included in the special class of offenses called "victimless crime," in which the "victims" either participate willingly or are habituated to the vice. The demand for gambling and narcotics has always existed, and in spite of the best efforts of law enforcement officials, it is unlikely that these vices will ever be eradicated. Gambling and narcotics are probably, at the same time, the primary source of income for many organized crime

families.

It is known that, between the two, wiretaps are more effective against gambling than against narcotics.[2] In the few state jurisdictions that have established a record of success in the use of wiretapping, for example New Jersey, the convictions as a direct result of wiretaps have been overwhelmingly in gambling cases. The one problem - or paradox - of gambling cases is that, in spite of the appropriateness of wiretaps, the offense is considered minor. Gambling convictions rarely justify the monetary expense of wiretaps,[3] as can be seen in the following table:

Reported sentences for gambling convictions as a result of wiretaps, for 1968 - 1973

More than 5 years.....1%
1 - 5 years.....21%
Less than 1 year.....20%
Discharge, fine, probation.....58%

Federal agencies have a far better record of success than state agencies in using wiretaps against narcotics. Indeed, there are glaring examples of state jurisdictions that have been unable to use wiretaps effectively against narcotics, even though they use them successfully against gambling.[4] The Federal experience in narcotics, however, is somewhat different from that of state agencies, because the distances involved in arranging certain interstate and many international narcotic deals occasionally make it necessary for criminals

to rely on telephone communication.[5] Even then, the telephone is used infrequently or not at all; or if used, it is often a public phone which is difficult to wiretap.[6] As a result, the Drug Enforcement Administration requests wiretap authority sparingly. Between 1968 and 1974, the DEA obtained 155 court authorizations, which ran an average of 18.5 days, and which resulted in the following reported sentences:[7]

Reported Sentences

More than 5 years.....29%
1 to 5 years.....22%
Less than 1 year.....12%
Discharge, fine, probation.....37%

2. Wiretaps used by state agencies have rarely been effective in obtaining evidence against the leaders or "bosses" of organized crime. The record of Federal agencies is characterized by a few exceptional successes and many fruitless efforts.

Most gambling wiretaps are used against small-time operators. This is also true for narcotics. Many law enforcement officials concede that organized crime bosses are too sophisticated to rely on the telephone to convey important information and are also cautious about conducting incriminating conversations in places where bugs can be installed. The exceptions in the Federal experience to this

generalization, however, are spectacular.* It is also clear from National Wiretap Commission studies, however, that wiretaps, if they do not lead to convictions, at least inconvenience or disrupt organized crime operations.

3. Most state jurisdictions that have wiretapping powers do not use them very often.

Twenty-seven of fifty states do not have wiretap statutes. Of those which do, New York and New Jersey together account for 70-80% of all state wiretaps installed.[8] The reasons for the infrequent use of wiretaps include high expenses, drain on manpower, paperwork, fear of evidence obtained through improperly implemented wiretaps being adjudged inadmissible,[9] inexperience in the handling of wiretaps, the effectiveness of other types of investigatory methods, personal dislike of wiretapping by certain prosecutors, and fear of public outcry.[10] The chart on the following pages summarizes the use of wiretaps during 1976 by jurisdictions.[11]

4. The Federal agencies in Hawaii rarely rely on wiretaps for non-national security cases.

---

*The National Wiretap Commission cites as examples the convictions of Dominic Brooklier of Los Angeles (extortion), Nicholas Civella of Kansas City (bookmaking), Frank Dasti of Montreal and New Jersey (narcotics), Sam DeCavlcante of New Jersey (gambling), and Joseph Columbo of New York (indicted for gambling, loan sharking and tax fraud before assassinated). Members of the Genovese family have also been convicted. Other non-mafia rings have been broken in Kansas City, Philadelphia, Pittsburg and Miami. National Wiretap Commission, Electronic Surveillance p. 140 (1976).

Major Offense for which Court-Authorized Intercepts were Granted Pursuant
To Title 18, United States Code, Section 2519, January 1, 1976 to December 31, 1976
(Concluded)

Reporting jurisdiction	Total	Arson and explosives	Bribery	Burglary	Escape	Forgery and Counterfeiting	Gambling	Homicide and assault	Kidnapping	Larceny and theft	Loansharking, usury and extortion	Narcotics	Obstruction of Justice	Possession, transport, or receipt of stolen property	Prostitution	Racketeering	Robbery
Minnesota																	
Anoka	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-
Nebraska																	
Douglas	4	-	-	-	-	-	3	-	-	-	-	1	-	-	-	-	-
Lancaster	2	-	-	-	-	-	-	1	-	-	-	1	-	-	-	-	-
New Hampshire																	
State Attorney General	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-
New Jersey																	
State Attorney General	44	-	-	-	-	-	30	-	-	-	-	14	-	-	-	-	-
Atlantic	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Bergen	3	-	-	-	-	-	1	-	-	-	-	2	-	-	-	-	-
Camden	7	-	-	-	-	-	2	-	-	-	-	5	-	-	-	-	-
Cape May	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-
Essex	39	-	-	-	-	-	32	-	-	-	-	6	-	-	1	-	-
Hudson	13	-	-	-	-	-	11	-	-	-	-	2	-	-	-	-	-
Mercer	5	-	-	-	-	-	-	-	-	-	-	5	-	-	-	-	-
Middlesex	13	-	-	-	-	-	5	-	-	-	-	8	-	-	-	-	-
Monmouth	1	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-
Morris	4	-	-	-	-	-	4	-	-	-	-	-	-	-	-	-	-
Ocean	2	-	-	-	-	-	1	-	-	-	-	1	-	-	-	-	-
Passaic	6	-	-	-	-	-	5	-	-	-	-	1	-	-	-	-	-
Somerset	9	-	-	-	-	-	5	-	-	-	-	3	-	1	-	-	-
Union	17	-	-	-	-	-	12	-	-	-	-	5	-	-	-	-	-
New York																	
State Attorney General	9	-	7	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Bronx	13	-	-	-	-	-	-	-	-	-	1	10	-	-	-	-	2
Chautauqua*	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Dutchess	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Erie	16	-	-	-	-	-	15	-	-	-	-	1	-	-	-	-	-
Kings	17	-	10	-	-	-	5	-	-	-	-	2	-	-	-	-	-
Monroe	3	-	-	-	-	-	1	1	-	-	-	1	-	-	-	-	-
Nassau	25	-	1	-	-	-	15	1	1	2	-	3	-	-	-	-	2
New York	17	-	5	-	-	-	-	-	-	-	2	10	-	-	-	-	-
Niagara	11	-	-	-	-	-	1	1	-	-	-	9	-	-	-	-	-
Onondaga	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Ontario	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Orange	2	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-
Queens	13	-	-	-	-	-	-	1	-	3	3	6	-	-	-	-	-
Rensselaer	11	-	-	-	-	-	11	-	-	-	-	-	-	-	-	-	-
Richmond	3	-	-	-	-	-	2	-	-	-	-	1	-	-	-	-	-
Rockland	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Schenectady*	6	-	-	-	-	-	6	-	-	-	-	-	-	-	-	-	-
Suffolk*	16	-	1	-	-	-	9	1	-	-	-	5	-	-	-	-	-
Sullivan	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Ulster	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Westchester	16	-	-	-	-	-	11	1	-	-	-	2	-	1	-	-	1
Rhode Island																	
State Attorney General	2	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	1
Washington																	
Kitsap	1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-
Wisconsin																	
Milwaukee	1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-

NOTE: This table shows generally the most serious offense for each court-authorized interception.
*No prosecutor's report.

Major Offense for which Court-Authorized Intercepts were Granted Pursuant
To Title 18, United States Code, Section 2519, January 1, 1976 to December 31, 1976

Reporting jurisdiction	Total	Arson and explosives	Bribery	Burglary	Escape	Forgery and Counterfeiting	Gambling	Homicide and assault	Kidnapping	Larceny and theft	Loansharking, usury and extortion	Narcotics	Obstruction of Justice	Possession, transport, or receipt of stolen property	Prostitution	Racketeering	Robbery
Total	686	4	24	-	1	1	378	10	1	9	17	190	1	10	2	30	8
Federal	137	2	-	-	-	1	53	-	-	1	6	36	1	5	-	30	2
Arizona																	
Maricopa*	11	-	-	-	-	-	9	-	-	2	-	-	-	-	-	-	-
Colorado																	
State Attorney General	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-
Second Judicial District	1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-
Connecticut																	
Fairfield	8	-	-	-	-	-	8	-	-	-	-	-	-	-	-	-	-
Hartford	4	-	-	-	-	-	1	-	-	-	-	3	-	-	-	-	-
Litchfield	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Middlesex	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Judicial District of Waterbury	2	-	-	-	-	-	1	-	-	-	-	1	-	-	-	-	-
Delaware																	
State Attorney General	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
District of Columbia	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Florida																	
State Attorney General	18	-	-	-	-	-	14	-	-	-	-	4	-	-	-	-	-
Sixth Judicial Circuit (Pasco & Pinellas Counties)	13	-	-	-	-	-	8	-	-	-	-	5	-	-	-	-	-
Ninth Judicial Circuit (Orange & Osceola Counties)	6	-	-	-	-	-	5	-	-	-	-	1	-	-	-	-	-
Eleventh Judicial Circuit (Dade County)	12	-	-	-	-	-	10	-	-	-	-	2	-	-	-	-	-
Seventeenth Judicial Circuit (Broward County)	24	-	-	-	-	-	18	-	-	-	1	3	-	1	1	-	-
Georgia																	
Bibb*	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Chatham	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-
Clayton	3	-	-	-	-	-	-	-	-	-	-	3	-	-	-	-	-
DeKalb	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Fulton	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Kansas																	
Johnson	3	-	-	-	-	-	-	-	-	-	-	3	-	-	-	-	-
Wyandotte	1	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Maryland																	
Anne Arundel	3	-	-	-	-	-	2	-	-	-	-	1	-	-	-	-	-
Baltimore City	25	-	-	-	-	-	21	-	-	-	-	4	-	-	-	-	-
Baltimore County	16	-	-	-	-	-	13	-	-	-	-	3	-	-	-	-	-
Charles	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Harford	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
Prince George's	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-
Worcester	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-
Massachusetts																	
State Attorney General	5	-	-	-	-	-	5	-	-	-	-	-	-	-	-	-	-
Plymouth	5	-	-	-	-	-	5	-	-	-	-	-	-	-	-	-	-
Suffolk	4	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-

Since 1968, Federal agencies in Hawaii have used only three court-ordered wiretaps. Federal officials cite the expense of wiretaps as the primary reason for the infrequency of its use.[12] Evidence obtained from those wiretaps, however, was critical in the prosecution of several organized crime figures.[13] And it should be said that, in spite of the rarity of its use, both the FBI and the Federal Strike Force of the United States Attorney's Office strongly believe in the effectiveness of wiretapping as an investigative tool.[14]

5. Wiretapping is an expensive operation.

The cost of a wiretap includes the value of plant and equipment, tapes, manpower - for repair and maintenance men as well as for detectives - and attorney time. Gambling cases are usually cheaper than narcotic cases because the tap is normally in operation for a portion of the day, whereas narcotics taps are likely to run all day and night for long stretches of time.[15] In New Jersey, the capital cost of wiretap equipment is $18,500.

Most jurisdictions that report costs of wiretap exclude the costs of preparing and filing an application, other attorney time and, sometimes, clerical time. With this in mind, the average reported cost of a state jurisdiction's wiretap is $8,482, with a range of $387 to $33,131. The average cost of a Federal wiretap is $19,223.[16] Judging from the analysis of cases in which wiretaps played a vital

role, the average cost is more like $10,000 to $20,000.

It is difficult for prosecutors to judge whether a wiretap will be cost-effective, owing to the problem of predicting when and where conversations yielding valuable information or evidence will take place.* Since most wiretaps are useful against gambling - and since gambling is a minor offense in most jurisdictions, resulting in sentences of rarely more than a year of actual prison time and often less - many prosecutors simply do not want to spend their funds on wiretaps.

6. There is some dispute as to whether evidence obtained from wiretapping has often been of critical importance in criminal prosecutions.

It is of doubtful value to simply correlate the number of wiretaps with the number of convictions in cases that used wiretaps, since it is not clear that the evidence obtained from wiretaps resulted in the conviction, or played a vital role in it. Nor is it clear that other investigative methods would not have yielded the same results. Each case must be examined individually - or, failing this, there should be an examination of a representative sample of cases. The

---

*The National Wiretap Commission found unproductive taps to be the rule in Colorado: Arapahoe County, Denver County and Garfield County; in Georgia: Fulton County; in Arizona: Maricopa County and Pima County; in Kansas; in Maryland: Prince George's County; in Minnesota: Hennpin County (Minneapolis) and Ramsey County (St. Paul); in New York: Queens County; Erie County (Buffalo), and Monroe County (Rochester). National Wiretap Commission, Staff Studies and Surveys (1976).

National Wiretap Commission undertook such an evaluation of representative samples. Their conclusions are much less supportive of wiretapping than the statistics would appear to show.[17]

7. An ancillary benefit of wiretapping is the collection of what is called "strategic intelligence."

Although a wiretap can be authorized only to intercept incriminating conversations concerning a particular offense, strategic information often will also be intercepted. Strategic intelligence is the bits and pieces of information which, put together, give a picture of the life of the suspect, for instance his personality, associations, habits, and life-style. Rarely is such information directly helpful in the prosecution of a particular case.[18] Before 1968, when the minimization principle - namely, the limiting of electronic eavesdropping only to matters relating to a particular criminal case - went into effect, Federal agencies used wiretapping to collect encyclopaedic information about organized crime figures. Such information was useful as a basis of planning an investigation or moving in new directions. Strategic intelligence wiretaps have been frequently used in national security cases. It has been occasionally used by state jurisdictions, but due to the minimization principle, the use of wiretapping to gather strategic intelligence is of doubtful constitutionality.[19]

III. PARTICULAR JURISDICTIONS AND CASES

Wiretapping has been useful - indeed indispensable - in many individual cases. These cases occur mainly in New York and New Jersey on the state and county levels, and in the work of Federal agencies in such places as New York, San Francisco, Philadelphia and Detroit. The following is a brief discussion of such exceptional jurisdictions and cases.

State of New Jersey

The Office of the Attorney General in New Jersey contains an Organized Crime and Special Prosecution Section which, with the aid of wiretaps, appears to have established a commendable record in prosecuting organized crime figures and corrupt officials. Consensual wiretapping is preferred in corruption cases, but court-authorized non-consensual electronic surveillance, especially bugs, has been used extensively in the investigation of criminals and to penetrate higher levels of organized crime.[20]

From 1969 to 1974, this section secured 330 indictments against 841 defendents, of whom 122 or 35% were indicted for gambling. About 20% were corruption cases, while 15% involved major thefts or robberies. The remaining one-third of the indictments included murder, narcotics, perjury, and prison riot. During this period the Section used 341

CONTINUED

1 OF 3

wiretaps.[21]

Number of Electronic Surveillance Orders, 1969-73: 318

Bribery and Corruption.....6
Escape.....1
Extortion.....9
Gambling.....231
Homicide.....6
Larceny and Receiving Stolen Goods.....27
Narcotics.....38

Number of Electronic Surveillance Orders, 1974: 23

Burglary, Larceny, and Stolen Property.....2
Burglary, Robbery, and Stolen Property.....1
Gambling.....11
Homicide.....1
Narcotics.....7
Narcotics, Burglary, Robbery, and Stolen Property.....1

New York County (Manhattan), N.Y.

The Manhattan District Attorney's office was under the direction of a single man, Frank S. Hogan, for over 30 years (until 1974) and has been esteemed as a model of sophisticated, incorruptible, non-political law enforcement. In recent years (since 1974), the office has been the target of some criticism and has undergone a more rapid turnover of personnel than was common in the past. Nonetheless, it remains a leader among local law enforcement agencies, especially in the use of electronic surveillance of organized criminal activity.

This prosecutorial agency has not only the most successful record in the use of wiretaps of any non-Federal agency, it also employs wiretaps effectively in a wide variety of investigations, including forgery, trafficking in stolen property and weapons, homicide, and extortion. Moreover, wiretapping is restricted to major cases and, apparently, does not supplant other investigative methods.

Number of Electronic Surveillance Orders, 1968-73: 251

Arson.....9
Bribery.....14
Burglary.....1
Escape.....1
Extortion.....11
Forgery.....5
Gambling.....42
Homicide.....24
Kidnapping.....1
Larceny, Robbery, Stolen Property.....63
Narcotics.....78
Obstruction of Justice.....1
Weapons.....1

Number of Electronic Surveillance Orders, 1974: 18

Extortion (Usury).....1
Extortion and Stolen Property.....2
Extortion, Stolen Property, and Larceny.....1
Grand Larceny and Extortion (Coercion).....2
Grand Larceny and Stolen Property.....2
Narcotics.....9
Weapons.....1

The following are examples of cases in which wiretapping played a key role in the investigation of major crimes:

CASE I

When the initial investigation provided probable cause to believe the suspect was involved in gambling and bribery of policemen, electronic surveillance was commenced. The electronic surveillance produced information which may have saved a witness at a federal trial from possible assassination; the surveillance also resulted in the disciplining of certain police officers. A spinoff tap on suspected gamblers was relatively unproductive. But, as a result of the entire investigation, thirteen persons were indicted for perjury or criminal contempt before a grand jury; according to an attorney directing the investigation, twelve persons were convicted, and one case is still pending. The major sentence meted out was four years imprisonment. The attorney stressed that when crime figures obey a code of silence and cannot be penetrated by undercover agents, the only successful tactic is to call the suspects before a grand jury, give them immunity, and confront them with the overheard conversations. The attorney also noted that this case was one that did not rely on informants; the case was made through physical surveillance and overheard conversations which required devoted police work. The attorney expressed doubts about the reliability of informants and believed that prosecutors should be wary of proceeding with cases based on such evidence; the attorney believed that electronic surveillance was one of the few ways to eliminate the reliance on informants in some types of conspiratorial cases.

CASE II

Another successful investigation concerned the investigation of a fencing ring. Beginning with a tap at the hangout of a suspected receiver of stolen goods, who apparently specialized in stolen traveler's checks, the investigators traced the scheme to persons to whom the receiver disposed of the checks. Taps on their phones led to an apartment where the stolen checks were delivered. A tap and bug were placed at this apartment. These electronic surveillances revealed information

as to burglaries, as well as fencing. Thirteen persons were arrested in all. Most have pled guilty; some are awaiting trial.

One rather unique investigation was designed to detect persons dealing in counterfeited phonograph records and tapes; that is, records and tapes bearing a label similar to that of the genuine manufacturer or distributor, in a case denominated as forgery investigation. Eight persons were arrested; four had their cases dismissed, and the other four pled guilty and received fines.[22]

Federal Agencies

The staff of the National Wiretap Commission found that Federal agencies - mainly the FBI, the Organized Crime Task Force and the Drug Enforcement Administration - have used wiretapping effectively in a number of important cases, though again it is clear that wiretapping is infrequently used except in gambling cases. The following, however, are examples of cases in which wiretaps were used effectively by a Federal agency:

CASE III

This case dealt with the Allen brothers - Aubrey Joe (A.J.) and Ambrey DeWitt (A.D.), who lived in the small town of Commerce, Georgia. Both brothers had extensive criminal records dating back to the mid-1940's for moonshining, Internal Revenue Law violations, and automobile theft. Both were also regarded as violence prone and extremely dangerous members of the Dixie Mafia.

In October 1972 an informant notified the FBI

that the Allen brothers and others working at their direction had been involved in a number of large thefts from clothing manufacturing plants in Georgia and South Carolina. The informant continued to provide such information until mid-January 1973, by which time he had provided the FBI with the details of 12 major burglaries, all of which were alleged to have been committed by the Allen gang. Through independent investigation, FBI agents were able to verify the facts of each of the 12 occurrences. In addition, this informant stated that the Allens were operating a large-scale fencing operation to dispose of the stolen merchandise and that they were using their home telephones to conduct these activities.

A second informant provided the FBI with the four telephone numbers used by the Allens (two in each of their residences) and substantiated the fact from personal knowledge, that both brothers were involved in theft and fencing operations in several southeastern states. A third informant stated that he had spoken with a number of persons who dealt in stolen clothing and had been told that they had bought the goods from A.D. Allen. A fourth informant had called A.D. Allen at a telephone number (the same as one of the four supplied by the first informant) and personally arranged for the purchase of stolen clothing.

Based on this information, the FBI decided to seek wiretaps on the Allens' telephones. The affidavit in support of the application detailed all of the informant information, as well as telephone toll records, which showed frequent calls by both Allen brothers to a number of persons throughout the southeast who were known by authorities to be dealing in stolen clothing. The affidavit also detailed why physical surveillance could not be used; both Allens lived in identical house trailers set high on a hill overlooking the only approach road to their property. In one instance where physical surveillance was attempted, the surveilling agents had been detected almost at once by A.J. Allen.

The 15-day wiretap order was signed on February 26, 1973. A leased line was provided by the telephone company and a monitoring post was

established at a motel near the Allens' property. Monitoring on two of the four lines was discontinued after a few days when it became apparent that no incriminating calls were being intercepted on those lines. A 15-day extension on the remaining two telephones was sought and granted on March 14. Because of a delay in getting approval for the extension, it was necessary to shut the taps down for one day, but once the order was signed monitoring began again and continued for a total of 28 days.

The results of the wiretap were excellent. Hundreds of incriminating conversations were intercepted, including several that enabled the FBI to locate two retail outlets that the Allens had established for the sale of their stolen goods. Search warrants were executed at the Allens' homes and 15 persons, including both Allen brothers, were later arrested.

Of those arrested, two pleaded guilty to reduced charges and one was dismissed. Twelve persons went to trial, where approximately 75 taped conversations were played for the jury. Four defendants were acquitted but eight were found guilty and were sentenced to prison terms ranging from 15 years (for both Allens) to two years.

The Allen case was a clear example of how a well-conceived wiretap can be used to attack a criminal conspiracy which may be immune from ordinary investigative techniques. Without electronic surveillance it is doubtful whether the major participants in this organization could have been convicted and the stolen goods located. It should also be noted that the fear which the informants expressed as a reason for not testifying in this case was apparently real. One witness who did agree to testify against the Allens was killed when his home was destroyed by a late night dynamite blast just a few days before the trial was to begin.

CASE IV

Wiretapping has also been used effectively in Atlanta against gambling organizations. One

case took place in 1971 and involved the lottery operation of Joe Dean Stanley and his associates.

Probable cause to seek wiretaps in the case came from informant information and limited physical surveillance. Beginning in January 1971, an FBI informant had revealed that Stanley, Hudson Ashley, and Henry "Jelly" Jones were the principals in a lottery operation in Atlanta grossing 10 to 15 thousand dollars a day. This informant also identified one woman who was operating a relay station for the lottery and provided her telephone number.

In February, a second informant substantiated this information and provided the FBI with the name and phone number of a second relay station operator. In May, this same informant provided a telephone number which Ashley was using to conduct lottery business.

A third informant was developed and, in July, he confirmed Stanley's role in the operation and provided his telephone number. A day later, informant No. 3 identified the main drag man for the Stanley organization.

During this period, FBI agents had surveilled the subjects on a number of occasions. The identified principals were observed meeting frequently at Stanley's home and the drag man was seen picking up small packages from the relay stations daily.

Finally, in mid-November 1971, all three informants confirmed their previous information as accurate and provided the further information that Stanley, in conjunction with a woman, was running a separate lay-off operation and taking lay-off bets from other lottery operators in Atlanta. The name and telephone number of the woman running this operation was provided.

Based on this information, a 15-day order authorizing wiretaps on four telephones (Stanley's, Ashley's and the two relay stations') was signed on November 24, 1971. Up to five days were required to install all of the taps because of inaccurate cable and pair information which was initially provided by the telephone company and the fact

that the FBI had only one agent trained to make the necessary connections. All of the taps were run over leased lines into a central monitoring post at FBI headquarters.

Incriminating conversations on each line were monitored from the start. In the case of one of the relay stations, so many incriminating calls were intercepted that the tap was shut down after just a few days because sufficient evidence had been gathered against the individual.

Because the lottery headquarters had not been located, 15-day extensions were sought on the remaining three wiretaps. In this case, as in the Allen case, the agents were forced to shut down the taps for two days because the extension order could not be signed before the original order expired.

Just two days after the extension was approved and the taps reinstalled, agents monitored a conversation between an unidentified caller and Ashley's wife, who was told, "you are hooked up all over". Later that day Ashley instructed the drag man, "don't talk on this line, it is tapped". Shortly thereafter, conversations on all three monitored lines ceased.

Despite this breach of security (which authorities attribute to a never-identified telephone employee), search warrants for the four tapped locations were secured and executed, resulting in the seizure of betting slips, $30,000 in cash (from Stanley's home), and the confiscation of three autos. (Lottery headquarters was never located.) Later, 37 individuals were indicted for their parts in the gambling operation, including all of the named participants except Stanley's alleged lay-off partner, against whom there was insufficient evidence.

Attempts to suppress the wiretap evidence were based on the alleged invalidity of the Attorney General's authorization. The resolution of this question dragged on for years, during which time Stanley and one other indicted individual died. When the signature question was later decided in the Government's favor, 26 defendants pleaded

guilty to Federal gambling violations. The remaining nine went to trial, at which seven were convicted and two were acquitted.

Unlike many gambling cases, most of the participants in this organization went to prison. Twenty-three persons were sentenced to terms ranging from 90 days to 10 years. The other 10 were placed on probation for three years.

In this instance, electronic surveillance was able to put an entire gambling organization out of business. Not all of the wiretap cases in Atlanta are this successful, of course. The FBI believes that one bookmaking operation closed up for two years after a number of wiretap-related arrests, but is now back in business. Although the problem is an ongoing one, the FBI's Ogden feels that wiretapping is the only tool which offers the potential for effective, sustained attacks on illegal gambling activity.[23]

IV. OVERVIEW

The effectiveness of electronic surveillance is partly determined by the importance that society attaches to the investigation of the crimes in which wiretaps are most useful. For example, the then Attorney General Mitchell considered it important to make a special effort to catch bookmakers. This resulted in frequent use of wiretaps in the years 1970-72 in "Project Anvil." Funds and other resources were allocated to this project in accordance with the Attorney General's judgment of the importance of prohibiting gambling, in preference to other needs in the criminal justice system. Wiretaps, of course, are most effectively used in the investigation of gambling cases. It can be seen that if the crime of gambling were to be given a lower priority -

or if organized criminal activities were to be relegated to a lower priority - the effectiveness of wiretapping, in so far as cost/benefit is considered, diminishes as the "benefit" side of the calculation diminishes. In the same way, if extortion or any other crime, in which wiretaps are marginally or occasionally useful, becomes such a danger to society that even marginally useful investigative tools are considered invaluable, it is possible that the effectiveness of wiretaps will be considered greater.

In summary, then, the Crime Commission and the Legislature must decide how much of a threat to society is posed by the crimes against which wiretaps are most effective, namely gambling, narcotics and organized criminal activities, and then measure that threat against the threat to individual privacy posed by wiretapping itself.

FOOTNOTES

CHAPTER V - EFFECTIVENESS OF WIRETAPPING

[1]See Administrative Office of the United States Courts, Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications, (hereafter cited as Report on Applications), Washington, D.C., 1973-1976.

[2]National Wiretap Commission, Staff Studies and Surveys, (hereafter cited as "Staff Studies and Surveys"), p. 177, Washington, D.C. (1976).

[3]National Wiretap Commission, Electronic Surveillance, (hereafter cited as "Electronic Surveillance"), p. 141, Washington, D.C. (1976).

[4]Staff Studies and Surveys, pp. 108-115. New Jersey is the most conspicuous example.

[5]Electronic Surveillance, p. 146.

[6]Ibid.

[7]Ibid., pp. 145-146.

[8]Herman Schwartz, Taps, Bugs and Fooling the People, New York, N.Y. 1977, p. 30.

[9]Electronic Surveillance, p. 127 (Interviews with law enforcement officials in Miami.); Staff Studies and Surveys, pp. 31 and 58 (Interviews with law enforcement in Connecticut and Georgia respectively.).

[10]Interviews with law enforcement officials in Colorado, in Connecticut, and in Georgia. Staff Studies and Surveys, pp. 22-23, 31, and 58.

[11]Report on Applications, pp. X-XI.

[12]Staff interview with Lee Laster, Special Agent-in-Charge, Honolulu Field Office, Federal Bureau of Investigation, July 26, 1977. Mr. Laster mentioned that for one wiretapping case 35 agents had to be brought in from the Mainland.

[13]Ibid.; Staff interview with U.S. Attorney Harold Fong, September 20, 1977.

[14]Ibid.; Staff interview with Michael Sterrett, Federal Strike Force Attorney, U.S. Dept. of Justice, Honolulu, September 20, 1977; and Staff interview cited in fN13 supra.

[15]Staff Studies and Surveys, pp. 121 and 124.

[16]Report on Applications, pp. XIV-XV.

[17]Staff Studies and Surveys, pp. 121 and 124. See also Ibid., pp.108-114 (Analysis of cases in New Jersey).

[18]Schwartz, op. cit., p. 31.

[19]For example, Niagara County, New York. Staff Studies and Surveys, p. 239.

[20]Staff Studies and Surveys, pp. 108-114.

[21]Ibid., p. 108.

[22]Ibid., pp. 300-301.

[23]Ibid., pp. 424-425.

CHAPTER VI

A MODEL WIRETAP STATUTE

I. INTRODUCTION

Generally, the model wiretap statute (see Appendix I) is similar to the Federal statute but incorporates added safeguards against unwarranted invasions of privacy. The most significant differences between the model statute and the Federal and most other state wiretapping statutes are the complete prohibition of court-ordered bugging, the use of an appointed attorney to oppose the wiretap application (the so-called "challenger"), the limitation of wiretap orders to very serious crimes or to other specific serious offenses when the involvement of organized crime is shown, the rigorous notice, disclosure, and destruction provisions, and a sunset provision that requires reenactment of the statute after eight years.

II. SCOPE

WIRETAPPING ONLY

The scope of the model statute is identical to that of the Federal statute and most other state wiretapping statutes except that court-ordered bugging is prohibited. The prohibition of court-ordered

bugging is a provision of House Draft 1 of House Bill 412, Ninth Legislature, State of Hawaii, 1977, and is designed to limit invasion of privacy. Although bugging is very similar to wiretapping in that both intercept private spoken conversations, bugging may involve a greater invasion of privacy. Bugging usually requires the placement of the bug inside or adjacent to the place being bugged. To the extent this involves a physical trespass it may be more of an invasion of privacy than wiretapping. Wiretapping can almost always be achieved by the use of telephone company facilities at telephone company offices. During a physical entry to place a bug, police officers investigating a crime would probably be tempted to observe as much as possible. Evidence found by the officers in "plain view" during the placement of a legal bug would be admissible in a criminal trial. Thus the temptation to conduct a general search or use a wiretap as a reason for entering a place to conduct a search might lead to even more extensive invasions of privacy.

Additionally, minimization is much more difficult in bugging than in wiretapping. Usually, only two persons are involved in a telephone conversation, and the persons involved usually identify themselves at the beginning of the conversation. Thus, it may be easier to determine the subject matter of a telephone conversation than that of oral conversations in a room where the parties to a conversation may change rapidly. Thus, telephone calls between persons not suspected of a wiretappable offense and involving a subject other than the offense

can be minimized. However, continuous monitoring of oral conversations may be believed to be necessary because it is impossible to tell when a conversation unlikely to contain incriminating statements begins or ends. With telephone conversations minimization is more readily accomplished. Monitoring equipment is triggered by the placing or receiving of a call. Monitoring officers determine if the two parties involved are likely to converse about the crime under investigation. If not, the monitoring equipment is shut off until the next telephone call. Finally, the prohibition of court-ordered bugging may be one way to limit invasions of privacy while still allowing some form of court-ordered interception of conversations. Thus, the model statute prohibits all wiretapping and bugging except court-ordered wiretapping and other exceptions set out below.

CONSENSUAL WIRETAPPING

The consensual exception for wiretapping as found in the Federal and most state statutes is included in the model statute. Consensual wiretapping is allowed without a court order with the consent of one of the parties to a conversation. However, bugging requires the consent of all parties entitled to privacy in the place bugged as under present law.[1] If one-party consensual bugging were allowed, extensive consensual bugging might make the prohibition of court-ordered bugging meaningless.

BUSINESS NECESSITY WIRETAPPING

For practical reasons of business necessity, exceptions for wiretapping by use of extension phones or party lines, by telephone companies, and by the Federal Communications Commission are retained in the model statute. It should be clarified that the exception for use of party line or extension phones applies only when the party line or extension phone is used by the person(s) to whom they are issued by the telephone company and is used in the normal course of business or operation.

OTHER AUTHORIZED WIRETAPPING

The model statute also does not prohibit wiretapping authorized by Federal law. This is considered necessary to avoid state interference with Federal supremacy.

III. COURT-ORDERED WIRETAPPING

The model statute allows court-ordered wiretapping by State officials with very strict regulation of the situations in which wiretap orders can be issued, the procedures and requirements for application, issuance, and execution of orders, and the protection of the privacy of intercepted conversations after the wiretap.

OFFENSES

Since the primary purpose of a wiretapping statute is to fight organized crime, the model statute requires that court-ordered wiretapping be allowed only in cases where organized crime is involved, except for a few very serious offenses.[2] Additionally, the model statute allows court-ordered wiretapping to be used only in the investigation of felony offenses which may involve use of telephone conversations. These severe restrictions are considered necessary since wiretapping is considered a substantial invasion of privacy and an extraordinary investigative tool to be used only in extraordinary cases. Thus, under the model statute the judge issuing the order must determine both (1) that organized crime is involved and (2) that a particular offense enumerated in the statute is being committed, except in the case of murder, kidnapping, and criminal property damage involving the danger of serious bodily injury.

ORGANIZED CRIME

Under the model statute, the application would usually be required to include facts which make it probable that organized crime is involved. The model statute includes a definition of organized crime which is a variation of the definition recommended by the Conference of State Governments and adopted by the Hawaii Legislature in the Organized Crime Act:

> *Organized crime is defined as any combination or conspiracy to engage in criminal activity as a source of income.*[3]

SPECIFIC OFFENSES

Wiretap orders may be issued in cases of murder, kidnapping and criminal property damage dangerous to persons without a showing of organized crime involvement. The model statute allows the use of wiretapping to investigate the following offenses when they are felonies and when organized crime is involved: bribery of a juror, witness or police officer; extortion; criminal coercion; receiving stolen property (fencing); gambling; and drug sales.

These specific offenses were chosen because they are thought to be characteristic of organized crime and may involve telephone communication. The offenses were limited to felony offenses in which organized crime is involved to ensure that wiretapping would only be used for serious offenses and to distinguish between small-time occasional gamblers, drug distributors, and fences and those likely to have connections with organized crime. In the case of small-time occasional offenses, the cost of wiretapping may not be justified and other investigative methods may be effective.

Several offenses included in House Draft 1 were changed to reflect proper Hawaii Penal Code titles for the offenses: arson was changed

to criminal property damage and corruption of public officials was changed to bribery of a witness, juror, or police officer. Bribery of a public official was not included in the offenses because of the potential for abuse of wiretap power for political purposes. Fencing or receiving stolen property under Hawaii law was added as a crime that is both characteristic of organized crime and may involve the use of the telephone. Some offenses included in House Draft 1 were deleted: prostitution, drug abuse, and loan sharking. Prostitution is probably not a wiretappable offense under the Federal wiretapping statute, since it is not a felony dangerous to life, limb, or property. Drug abuse is neither a crime nor is it characteristic of organized crime. Rather, it is believed that organized crime is involved in drug sales, which is a wiretappable offense under the model statute. Finally, loan sharking is deleted from the model statute because there is no comprehensive Hawaii law regulating loan sharking. Criminal coercion, included in the model statute, may cover most extortionate lending practices. If the Hawaii Legislature does enact comprehensive regulation of loan sharking similar to the Federal Extortionate Credit Act,[4] then it should be considered by the Legislature for inclusion as an offense for which wiretapping orders may be issued.

WHO MAY APPLY

The model statute adopts an application procedure similar to that of the Federal statute. The Attorney General and the chief prosecuting attorney of each county may apply for wiretap orders. The model statute contemplates that the county prosecuting attorney or the

Attorney General would apply in person for the wiretap order. Allowing application by deputies with the authorization of the prosecuting attorney or Attorney General might result in "rubber stamp" approval. Wiretapping is designed for infrequent use in extraordinary situations so that requiring the applicant to appear in person when not absent from the State or incapacitated should not be an undue burden.

WHO MAY ISSUE

The Federal statute allows a state to empower any judge of "general criminal jurisdiction" to issue wiretap orders.[5] General criminal jurisdiction probably means jurisdiction over criminal hearings, trials or appeals of all levels and kinds of offenses. This would probably exclude Hawaii district court judges since they have limited criminal jurisdiction. Generally, district court judges have misdemeanor (non-felony cases) criminal jurisdiction and jurisdiction only over arraignments, preliminary hearings, and issuance of search and arrest warrants in felony cases. Circuit court judges have general criminal jurisdiction over all criminal cases and, thus, could be empowered to issue wiretap orders.

The model statute allows a designated circuit court judge in each circuit to issue a wiretapping order. The Chief Justice of the Supreme Court is required to appoint a judge in each circuit to hear wiretap applications. This should prevent "forum shopping" for favorable judges.

STANDARDS FOR ISSUING ORDERS

The standards for issuing orders set by the model statute are identical to those required by the Federal statute except that no court-ordered bugging is allowed and the application and order must specify whether physical entry is necessary to accomplish the wiretap. This is designed to prevent physical entry unless it is absolutely necessary. Most wiretaps can be accomplished by use of telephone company facilities without physical entry.

EMERGENCY WIRETAPS

The model statute allows no emergency wiretaps. All wiretaps require a court order. Most other state statutes do not allow emergency wiretapping. Emergency wiretaps have been criticized because there is no judicial control over law enforcement officers in initiating and conducting the wiretap. Wiretapping is believed to be too great an invasion of privacy without the safeguards imposed by judicial supervision of the wiretap at all stages. Unlike the Federal procedures for application, State law enforcement officers seeking a wiretap need not seek approval from Washington, D.C. Thus, the application process in the model statute should be much quicker than the Federal procedure. This should eliminate the need for emergency wiretaps in many cases.

CHALLENGER PROVISION

The model statute provides for an adversary hearing on an application for a wiretap order. In an adversary hearing, opposing attorneys present facts and argue different sides of an issue(s) before a judge. It is often believed that the search for truth and justice is best accomplished through an adversary hearing. Normally, a hearing for the issuance of search or arrest warrants is ex parte, meaning that only one side of the case is presented to the judge. This ex parte procedure is employed in wiretap applications under the Federal and other state statutes. Opposition by an attorney representing the public will provide the best possible protection against "rubber stamping" by judges, or decisions based on a distorted one-sided view of the evidence and arguments supporting an application.

Like other rigorous procedures that further protect privacy, an adversary hearing will result in some additional costs and delay. However, because wiretapping will be used infrequently and because it may result in a substantial invasion of privacy, the added costs are considered justified.

The attorney to represent the public by opposing the application should be appointed by the circuit court judge hearing the application on a case-by-case basis. The circuit court judge may appoint a government attorney, such as the public defender, or a private attorney.

Any private attorney appointed should be compensated on an hourly basis at the same rate as other court-appointed attorneys.

The hearing itself would be held in secret in the judge's chambers to protect the confidentiality necessary to a successful wiretap. The attorney should have the right to cross-examine the affiant supporting the application and to present arguments in opposition to the application. In order to do this effectively, the attorney must be allowed to read the application and supporting documents prior to the hearing and then prepare for the hearing. Twenty-four hours notice and discovery to an opposing attorney is required by the model statute. This should be adequate notice to ensure that the attorney opposing the application can do so effectively and still allow law enforcement to move swiftly.

DURATION OF WIRETAP

The model wiretap statute, like the Federal statute, allows wiretaps to be conducted for a maximum of 30 days and allows extensions of 15 days each. Although organized crime is believed to be conducting criminal activity, such as gambling, on a daily basis, contacts with the leaders of organized crime may occur less often. Thirty days is believed to be a sufficient period to intercept these contacts between lower-level criminal operators and high-level leaders of organized crime. Additionally, anything less than 30 days would probably result in increased applications for extensions at added costs.

Application for extensions must follow the same procedures as that for original applications. Also, as in the Federal statute, "fresh" probable cause must be shown in addition to an explanation why the wiretap should be continued. Extensions of shorter periods of 15 days each are allowed because a failure of the wiretap during the original period may question the justification for as substantial an invasion of privacy as an additional 30 days.

However, all wiretaps must automatically terminate if the evidence sought is obtained. This requirement is mandated by the Federal and Hawaii Constitutions and the Federal wiretap statute. Automatic termination has been criticized as an unworkable concept since it is difficult to decide whether a particular intercepted statement is the type of communication described in the wiretap order and since a law enforcement officer interested in obtaining as much evidence as possible must make this decision. The model statute provides for an immediate report to the issuing judge when an incriminating statement is obtained. This allows a neutral judge, rather than the law enforcement officers involved, to decide whether the statement intercepted is the type of statement sought by the wiretap. This is designed to ensure that automatic termination occurs.

MINIMIZATION

The Federal and Hawaii Constitutions and all wiretap statutes

require that wiretapping be done in such a way as to minimize the invasion of privacy. The model statute includes this general requirement and also specifies some methods of minimization. The first method of minimization recognized by Federal and other state law enforcement officials is monitoring only those conversations likely to contain incriminating conversations. The statute also sets out some factors to be considered in determining whether a conversation is likely to result in incriminating statements. These factors are the parties involved; the initial subject matter of the conversation; the particular offense under investigation; the subject matter of previous conversations between the same parties and whether incriminating statements were made; and the time and day of the particular conversation.

Because it is difficult to determine in advance whether a particular conversation will contain incriminating statements, other means of minimization are also specified. Only conversations involving at least one person who is named or described in the wiretap application and order may be monitored. For example, if the wiretap order names Joe Gambler and establishes probable cause that he is conducting a gambling operation, any telephone call Joe makes or receives may be monitored. However, if Joe Gambler's daughter calls her boyfriend, then the conversation cannot be intercepted. This limits the invasion of privacy to persons about whom there is probable cause that they are committing a crime and those who converse with them by telephone. It

may still result in guilt by association, as does all wiretapping where probable cause is not required for each party to a conversation. However, with this requirement persons about whom there is no probable cause who happen to use a telephone that is wiretapped do not have their privacy invaded.

The final method of minimization expressly included in the statute is the protection of privileged conversations, such as conversations between a person and his spouse, doctor, attorney or clergyman. The law of evidence has traditionally recognized these conversations as being very important and confidential. Since these conversations would not usually be admissible in a court proceeding, there is no justification for intercepting this type of conversation except when the conversations are not privileged, when both parties to the conversation are involved in the commission of a crime. Thus, the model statute would allow interception of these conversations only when there is probable cause to believe that both parties are involved in the commission of the named offense.

As the statute implies, and as the Hawaii and Federal Constitutions require, the execution of the wiretap must be in such a way as to minimize the invasion of privacy, which in certain circumstances may require more than the specific methods of minimization included in the statute.

REPORTS TO THE JUDGE

The model statute allows the issuing judge to determine if and when reports on the progress of the wiretap should be made by the officers conducting the tap. The challenger may make it likely that a judge will require such reports. However, it is considered unwise for the statute to require periodic reports in every wiretap since it may be burdensome for law officers to prepare and for judges to review several days of recorded conversations while the wiretap is still being conducted. Additionally, reports are required whenever an incriminating statement is obtained.

NOTICE OF THE WIRETAP

The model statute suggests that notice be given to all known persons whose conversations were intercepted and to any person(s) named in the wiretap order. Notice to everyone whose privacy is invaded is considered fair and necessary to deterring illegal wiretapping. Without such notice a person may not know of the invasion of privacy and cannot further investigate to determine its legality, consider a civil suit, or urge prosecution by the State if the wiretap appears to have been an illegal one. Because notice is required only to known parties, the burden on the courts or law enforcement should not be too great. The parties must be identified anyway before the conversations can be useful to law enforcement.

The statute requires notice to be given within 90 days, but allows a judge to extend the time if there is a good reason for doing so. Because wiretap investigations may be complex and may require additional follow-up investigation after the wiretap is completed, the model statute follows the Federal and most state statutes in allowing 90 days and possible extensions. However, the model statute requires notice immediately upon the arrest or indictment of a person for an offense in which there is wiretap evidence. At the time that an arrest is made or a public indictment is obtained, any investigation relating to the person arrested is probably already public and already completed, so that few reasons remain for keeping the wiretap secret. At the time of arrest or indictment, an accused should be told of the use of the wiretap so that he can investigate and prepare his defense.

The notice must contain the fact that a wiretap was conducted, the dates and duration of the wiretap, whether any conversations were monitored and whether incriminating statements were obtained. The Federal statute also requires notice of whether an application for a wiretap order was denied. The model statute does not require notice of this since no invasion of privacy results when an application is denied, and since law enforcement may again apply for a wiretap involving the same person when additional evidence is obtained. Notice to a person of a prior unsuccessful application might make a subsequent wiretap on that person ineffective, since he could purposefully avoid incriminating conversations.

DISCLOSURE

The model statute makes the disclosure of the application, order, and a person's intercepted conversations mandatory upon request of any person whose conversations are intercepted. The disclosure occurs after notice has been given but at least 30 days before any trial in which the wiretap evidence is to be used. Any person intercepted has the right to sue civilly or to seek criminal prosecution if the wiretap was illegal. A person cannot determine the legality of the wiretap without seeing the application, the order, and the contents of his or her intercepted communications. Since this would occur after notice, there should be no compelling reasons to keep the application, the order, or the contents secret.

It should be noted that a person can only see intercepted conversations to which he was a party. Otherwise, any person intercepted might be able to see conversations of other people which should remain as confidential as possible. A person should be able to see his conversations both to evaluate the legality of the wiretap and plan a criminal defense if prosecution appears likely. A person's intercepted conversations may be relevant to the legality of the wiretap, for example, because they can show the absence of required minimization. If incriminating statements are intercepted, a person should be able to see them in order to plan a possible defense. Currently, Hawaii's Rules of Criminal Procedure require that an accused be allowed to view

any statements he or she made to law enforcement concerning the crime.[6]

INTERLOCUTORY APPEAL

The model statute allows appeal by the applicant upon the denial of an application and upon granting of a motion to suppress any wiretap evidence in a criminal case. In the case of denial of an application, no one is prejudiced by the appeal and a judge's decision whether to allow a wiretap should, like other judicial decisions, be subject to review. Immediate appeal does not prejudice anyone involved and may allow a decision before the opportunity to intercept incriminating conversations is lost.

Interlocutory appeal from the granting of a motion to suppress is probably already allowed by Hawaii law.[7] The model statute expressly allows it to ensure that it is allowed in wiretap cases. Interlocutory appeal is necessary because the State cannot take a normal appeal at the end of the case. If the State wins a conviction there is nothing for it to appeal. If the State loses, it cannot try the defendant again because of the prohibition against putting a person twice in jeopardy for the same criminal offense.

Although interlocutory appeal from the suppression of evidence is allowed, the model statute requires that the appeal be filed as soon as possible and that the issue be decided as rapidly as possible

in order to protect the defendant's right to a speedy trial. Generally, trial is required to begin within six months after arrest or indictment in Hawaii.[8]

IV. PROHIBITING UNAUTHORIZED WIRETAPS

Like the Federal and most state statutes, the model statute seeks to prevent unauthorized wiretapping and bugging by criminal penalties, civil suits, and exclusion of illegally obtained wiretap evidence.

CRIMINAL LIABILITY

Like the Federal and all state statutes, the model statute makes criminal the illegal or unauthorized interception, use, or disclosure of private conversations and the possession, manufacture, or distribution of wiretap devices. Confiscation of illegal devices is allowed. Finally, the telephone company is required to report all wiretaps of which it has knowledge as a check on illegal wiretaps that might be conducted without proper court authorization.

A good faith reliance upon a court order is made a complete defense to any criminal charge. A telephone company employee or a law enforcement officer executing the wiretap pursuant to a court order should not be criminally liable when it appears that the court order

is illegal because of something the employee or law enforcement officer did not do and did not know about.

A maximum criminal penalty of $5,000 and a five-year prison term is thought appropriate, since higher penalties might deter the judge from giving a prison sentence. In Hawaii, a judge must give the maximum if he gives any prison sentence; then the parole board determines eligibility for early parole.[9]

CIVIL SUIT

The model statute allows a civil suit for illegal invasion of privacy and recovery of actual damages or $100 a day, whichever is greater, court costs including reasonable attorney's fees, and punitive damages if malice is shown. Unlike the Federal and many state statutes, the model statute does not provide a minimum recovery of $1,000. Presumably, a minimum recovery would be allowed to any person whose conversation was intercepted in an illegal wiretap regardless of the length, number, and nature of the conversations. Since one wiretap may involve the conversations of many people, a minimum recovery of $1,000 might place a financial hardship on the State. $100 a day or actual damages, plus the costs of suit are considered sufficient to encourage civil suits which deter illegal wiretapping and compensate the victim of illegal wiretapping.

Good faith reliance upon a court order is also a defense to civil liability on the part of an individual for the same reasons that it is made a defense to criminal liability. However, the model statute does not allow good faith as a defense to liability on the part of the State. Any illegal wiretap is still an illegal invasion of privacy regardless of good faith and the victim should be compensated.

EXCLUSION OF EVIDENCE

The model statute provides for exclusion of evidence obtained as a result of an illegal wiretap, as is required by both Federal and State laws.

ANNUAL REPORTS ON WIRETAPS

The model statute also requires that applicants for and judges hearing applications for wiretaps report to the Administrative Director of Hawaii Courts the information required to be reported to the Federal authorities by the Federal statute. In turn, the Administrative Director must report to the Legislature concerning wiretaps. This will allow Hawaii to judge the effectiveness of wiretapping and does not require additional data beyond that required for Federal reports.

SUNSET PROVISION

Finally, the model statute provides a sunset provision that pro-

vides that the wiretapping statute automatically expire in eight years. A commission is to be appointed at the end of five years to study wiretapping in Hawaii. The commission must report to the Legislature before the statute expires so that the Legislature can make an informed decision as to whether court-ordered wiretapping should be continued in Hawaii.

The sunset provision is a recognition that the effectiveness and effect of wiretapping are not accurately known and that such a substantial invasion of privacy should not continue unless it is effective in fighting crime. Because it is perhaps more difficult to repeal an existing law than to pass a new one, a sunset provision is considered prudent.

V. CONCLUSION

The model statute is designed to allow court-ordered wiretapping to fight organized crime in Hawaii, while protecting privacy to the fullest extent possible without crippling law enforcement efforts. In order to do this, the model statute includes more rigid procedures and protections of privacy than perhaps any other state or Federal statute. The use of an adversary attorney to challenge applications; the requirement that a showing of the involvement of organized crime be made in most cases; the specified methods of minimization required; and several other statutory provisions are unique and are designed to meet many of

the criticisms of the Federal statute and other state statutes modeled after the Federal statute.

ADDENDUM

The model statute described in this Chapter and contained in Appendix I was introduced in the 1978 Hawaii Legislature. The legislature passed the wiretap bill with a few substantive changes. The substantive changes are as follows:

1) the definition of organized crime was changed from "...any combination or conspiracy to engage in criminal activity as a source of income" to "...any combination or conspiracy to engage in criminal activity";
2) the requirement in the model bill that only communications in which one party was named in the wiretap order could be monitored was deleted;
3) the minimization provision allowing initial monitoring of a telephone conversation to determine if the conversation is likely to result in incriminating statements was modified to allow intermittent monitoring to determine if incriminating statements are likely;
4) the reporting requirement in the model bill requiring immediate reports of the interception of incriminating statements was changed to require periodic reports to the issuing judge concerning the wiretap;
5) a good faith belief in a court-order was made a defense to civil liability of the state, as well as individuals for illegal wiretapping; and
6) the sunset provision gives the wiretap law a life of six years rather than eight years as specified in the model statute.

The legislature also made a few non-substantive changes in wording. The statute with the legislative changes is still more protective of individual privacy than the federal statute or most other state wiretap statutes.

FOOTNOTES

CHAPTER VI - A MODEL WIRETAP STATUTE

[1]Hawaii Revised Statutes ("H.R.S.") §711-1111 (1976).

[2]House Bill 412, House Draft 1 adopts the same requirement.

[3]Council of State Governments, 1971 Suggested State Legislation XXX 43-30-00 (1970); H.R.S. §842-1 et.seq. (1976).

[4]18 United States Code ("U.S.C.") §891 et.seq. (1968).

[5]18 U.S.C. §§2510(9) and 2516(2) (1968).

[6]Rule 16(b)(ii), Hawaii Rules of Penal Procedure (1977).

[7]H.R.S. §641-13 (1976).

[8]Rule 48(b), Hawaii Rules of Penal Procedure (1977).

[9]H.R.S. §§706-605 and 706-660 (1976).

APPENDIX I

TEXT OF THE MODEL WIRETAP STATUTE

The text of the model statute follows. The model statute is an amended form of House Bill 412, House Draft 1 (H.D. 1), Ninth Legislature, State of Hawaii, 1977, which in turn was modeled upon the Federal wiretap statute.

(To be made one and ten copies)

HOUSE OF REPRESENTATIVES
NINTH LEGISLATURE, 1978
STATE OF HAWAII

H.B. NO.

A BILL FOR AN ACT

RELATING TO ELECTRONIC EAVESDROPPING

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Purpose.

(1) In order to protect effectively the privacy of wire and oral communications while fighting organized crime and to protect the integrity of court and administrative proceedings, it is necessary for the Legislature to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of wire and oral communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

(2) Organized criminals make extensive use of wire communications in their criminal activities. The interception of such communications to obtain evidence

of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

(3) To safeguard the privacy of innocent persons, the interception of wire communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire communications should further be limited to the most serious offenses and less serious offenses only when organized crime is involved, with assurances that the interception is justified and that the information obtained thereby will not be misused.

SECTION 2. Chapter 803, Hawaii Revised Statutes is amended by adding a new part to read as follows:

"PART IV. ELECTRONIC EAVESDROPPING.

Sec. 803-41 Definitions. In this part:

(1) "Wire communication" means any communication 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 furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications;

(2) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

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

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

(a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary

course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

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

(5) "Person" means any official, employee, or agent of the United States or this State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(6) "Investigative or law enforcement officer" means any officer of the State or political subdivision thereof, who is empowered by the law of this State to conduct investigations of or to make arrests for offenses enumerated in this part;

(7) "Contents" when used with respect to any wire communication, includes any information concerning the identity of the parties to such communication or

the existence, substance, purport, or meaning of that communication;

(8) "Organized crime" means any combination or conspiracy to engage in criminal activity as a source of income;

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

Sec. 803-42 Interception and disclosure of wire or oral communications prohibited.

(1) Except as otherwise specifically provided in this part any person who:

(a) Wilfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

(b) Wilfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any wire or oral communication;

(c) Wilfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through

the interception of a wire or oral communication in violation of this subsection; or

(d) Willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;

shall be guilty of a class C felony.

(2) (a) It shall not be unlawful under this part for an operator of a switchboard, or an officer, employee, or agent of any communications common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication; provided that such communications common carriers shall not utilize service observing or random

monitoring except for mechanical or service quality control checks.

(b) It shall not be unlawful under this part for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this part for a person to intercept a wire or oral 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 this State or for the purpose of committing

any other injurious act; provided that installation in any private place, without consent of the person or persons entitled to privacy therein, of any device for recording, amplifying, or broadcasting sounds or events in that place, or use of any such unauthorized installation, or installation or use outside a private place of such device to intercept sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein is prohibited.

(d) It shall not be unlawful under this part for any person to intercept a wire or oral communication or to disclose or use the contents of an intercepted communication, when such interception is pursuant to a valid court order under this chapter or as otherwise authorized by law; provided that a communications carrier with knowledge of an interception of communications accomplished through the use of the communications carrier's facilities shall report

the fact and duration of the interception to the administrative director of the courts of this State.

(e) Good faith reliance upon a court order shall be a complete defense to any criminal prosecution for illegal interception, disclosure, or use.

Sec. 803-43 Devices to intercept wire or oral communications prohibited; penalty; confiscation. Any person, other than a communications or other common carrier and its duly authorized officers and employees, or any person acting under color of law, who, in this State, manufactures, assembles, possesses, or distributes, or who attempts to distribute, any electronic, mechanical, or other device, knowing or having reason to know that the device or the design of the device renders it primarily useful for the purpose of wiretapping, wire interception, or eavesdropping, shall be guilty of a class C felony. Any police officer may confiscate any such electronic, mechanical, or other device in violation of this section, and upon conviction the devices shall be destroyed or otherwise disposed of as ordered by the court.

Sec. 803-44 Application for court order to intercept communications. The attorney general of this State, or a designated deputy attorney general in the attorney general's absence or incapacity, or the prosecuting attorney of each county, or a

designated deputy prosecuting attorney in the prosecuting attorney's absence or incapacity, may make application to a circuit court judge, designated by the chief justice of the Hawaii supreme court in the county where the interception is to take place, for an order authorizing or approving the interception of wire communications, and such court may grant in conformity with section 803-46 an order authorizing, or approving the interception of wire communications by investigative or law enforcement officers 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 murder, kidnapping, or felony criminal property damage involving the danger of serious bodily injury as defined in H.R.S. Section 707-700(3), or involving organized crime and any of the following felony offenses: extortion; criminal coercion; bribery of a juror, of a witness, or of a police officer; receiving stolen property; gambling; and sales of dangerous, harmful or detrimental drugs.

Sec. 803-45 Authorization for disclosure and use of intercepted wire communications. (1) Any investigative or law enforcement officer who, by any means authorized by this part, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may 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.

(2) Any investigative or law enforcement officer, who by any means authorized by this part, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this part, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this part may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding in any court or before the grand jury in this State.

(4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this part shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized, intercepts communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section.

Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by the designated circuit court where such court finds on subsequent application, made as soon as practicable, that the contents were otherwise intercepted in accordance with the provisions of this part.

(6) No testimony or evidence relating to a wire or oral communication or any evidence derived therefrom intercepted in accordance with the provisions of this part shall be admissible in any proceeding for any misdemeanor charge.

Sec. 803-46 Procedure for interception of wire communications. (1) Each application for an order authorizing or approving the interception of a wire communication shall be made in writing upon oath or affirmation to a designated circuit court and shall state the applicant's authority to make such application. Each application shall include the following information:

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

(b) A full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be

issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity or description of all persons, if known, committing the offense and whose communications are to be intercepted, and (v) the involvement of organized crime;

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

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

(e) A statement of facts indicating the period of

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

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

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

(2) An in camera adversary hearing shall be held on any wiretap application or application for extension. Upon receipt of the application the designated judge shall appoint an attorney to oppose the application. The attorney shall be appointed and compensated in the same manner as attorneys are appointed to represent indigent criminal defendants. The appointed attorney shall be given at least twenty-four hours notice of the hearing and shall be served with copies of the application, proposed order, if any, and supporting documents with the notice. At the hearing, the attorney appointed may cross-examine witnesses and present arguments in opposition to the application. The affiant supporting the application shall be present at the hearing. If an interlocutory appeal is taken by the State from the denial of an application, the appointed attorney shall be retained to answer the appeal or another attorney shall be appointed for the appeal. The designated circuit court may require the applicant to furnish additional testimony or documentary evidence under oath or affirmation in support of the application. A transcript of the hearing shall be made and kept with application and orders.

(3) Upon such application the court may enter an order, as requested or as modified, authorizing or approving interception of wire communications within the county in which the court is sitting, if the court determines on the basis of the facts submitted by the

applicant that:

(a) There is probable cause for belief that an individual is committing, has committed, or is about to commit murder, kidnapping, or felony criminal property damage involving the danger of serious bodily injury or that an individual is committing, has committed, or is about to commit one of the other offenses specified in section 803-44 and that organized crime is involved;

(b) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and

(d) There is probable cause for belief that the facilities from which, or the place where, the wire communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense,

or are leased to, listed in the name of, or commonly used by such person.

If the order allows physical entry to accomplish the interception, the issuing judge shall find that the interception could not be accomplished by means other than physical entry.

(4) Each order authorizing or approving the interception of any wire communication shall specify:

(a) The identity or description of all persons, if known, whose communications are to be intercepted;

(b) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and the means by which such interceptions shall be made;

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

(d) The identity of the agency authorized to intercept the communications and the persons applying for the application;

(e) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically

terminate when the described communication has been first obtained; and

(f) How the interception is to be accomplished.

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

(5) No order entered under this section shall authorize or approve the interception of any wire communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsections (1) and (2) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing circuit court deems necessary to achieve

the purposes for which it was granted and in no event for longer than fifteen days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this part, and shall terminate upon attainment of the authorized objective, or in any event in thirty days or in fifteen days in case of an extension.

(a) The interception shall be conducted in such a way as to minimize the resulting invasion of privacy including but not limited to the following methods of minimization:

(i) Conversations that appear unlikely to result in incriminating conversations relating to the offense for which the order is issued shall not be intercepted;

(ii) Conversations, in which none of the persons involved are named or described in the application and order shall not be intercepted; and

(iii) Privileged conversations, including those between a person and his spouse, attorney, physician, or clergyman, shall not be intercepted unless both parties to the conversation are named or described in the wiretap application and order.

(b) In determining whether incriminating statements are likely to occur during a conversation the following factors should be considered:

(i) The parties to the conversation;

(ii) The particular offense being investigated;

(iii) The initial subject matter of the conversation;

(iv) The subject matter of previous conversations between the same parties and whether any incriminating statements occurred; and

(v) The hour and day of the conversation.

(6) Whenever an order authorizing interception is entered pursuant to this part, the order may require reports to be made to the court which issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the court may require. In addition, reports of the interception of incriminating statements shall be made as soon as practicable after such interception in order for the issuing judge to decide whether the interception should automatically terminate.

(7) (a) The contents of any wire communication intercepted by any means authorized by this part shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire 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 court issuing such order and sealed under the court's directions. Custody of the recordings shall be wherever the court orders. Recordings and other evidence of the contents of conversations and applications and orders shall be destroyed upon the expiration of the statute of limitations for the particular offense for which the order was issued: six years in the case of class A felonies and three years in the case of class B and C felonies. However, upon the request of all the parties to particular conversations, evidence of conversations between those parties shall be destroyed (i) if there are no incriminating statements; (ii) if any incriminating statements relate to misdemeanor offenses; or (iii) if the interception of the conversations is determined to have been illegal. Duplicate recordings may be made for use or disclosure pursuant to the provisions of sections 803-45(1) and (2) 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 communication or evidence derived therefrom under section 803-45(3).

(b) Applications made and orders granted under this part, transcripts of hearings on applications, and evidence obtained through court-ordered wiretaps shall be sealed by the designated circuit court. Custody of the above shall be whenever the court directs.

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

(d) Within a reasonable time but no later than ninety days after the termination of the period of an order or extensions thereof or upon arrest or indictment of a person who has been wiretapped, whichever comes sooner, the issuing court shall cause to be served, on the persons named in the order, on all other known parties to intercepted communications, and to such other persons as the court may determine is in the interest of justice, an inventory which shall include notice of:

(i) The fact of the entry of the order;

(ii) The date of the entry and the period of authorized, or approved interception;

(iii) The fact whether during the period wire communications were intercepted; and

(iv) The fact whether any incriminating statements were intercepted.

The designated circuit court, upon the filing of a motion, shall make available to such person or his counsel for inspection after the inventory has been served all portions of the intercepted communications which contain conversations of that person, applications, orders, transcripts of hearings, and other evidence obtained as a result of the use of wiretap orders. The court may order such additional disclosure as the court determines to be in the interest of justice. On an ex parte showing of good cause to a court the serving of the inventory required by this subsection may be postponed.

(8) The contents of any intercepted wire communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in any court of this State unless each party, not less than thirty

days before the trial, hearing, or proceeding, has been furnished with copies of the documents required to be disclosed, and contents of intercepted communications or other evidence obtained as a result of wiretapping which is sought to be admitted in evidence. This thirty-day period may be shortened or waived by the court if it finds that it was not possible to furnish the party with the above information thirty days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(9) (a) 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 intercepted wire communication, or evidence derived therefrom, on the grounds that:

(i) The communication was unlawfully intercepted;

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

(iii) The interception was not made in conformity with the order of authorization or approval. Such motion shall be made before the trial,

hearing, or proceedings 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 communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this part. The court, or other official before whom the motion is made, upon the filing of such motion by the aggrieved person, shall make available to the aggrieved person or his counsel for inspection portions of the recording which contain intercepted communications of the defendant or evidence derived therefrom, the applications, orders, transcript of hearing, and such additional evidence as the court determines to be in the interest of justice.

(b) In addition to any other right to appeal the State shall have the right to appeal:

(i) From an order granting a motion to suppress made under paragraph (a) of this subsection if the attorney general or prosecuting

attorney, or their designated representatives, shall certify to the court or other official granting such motion that the appeal shall be taken within thirty days after the date the order of suppression was entered and shall be diligently prosecuted as in the case of other interlocutory appeals or under such rules as the supreme court may adopt;

(ii) From an order denying an application for an order of authorization or approval, and such an appeal shall be in camera and in preference to all other pending appeals in accordance with rules promulgated by the supreme court.

Sec. 803-47 Reports concerning intercepted wire communications.

(1) In January of each year, the attorney general and county prosecuting attorneys of this State shall report to the administrative director of the courts of this State and to the administrative office of the United States Courts:

(a) The fact that an order or extension was applied for;

(b) The kind of order or extension applied for;

(c) The fact that the order or extension was granted as applied for, was modified, or was denied;

(d) The period of interceptions authorized by the

order, and the number and duration of any extensions of the order;

(e) The offense specified in the order or application, or extension of an order;

(f) The identity of the investigative or law enforcement officer and agency requesting the application and the person authorizing the request for application;

(g) The nature of the facilities from which or the place where communications were to be intercepted;

(h) A general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

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

(j) The number of trials resulting from such interceptions;

(k) The number of motions to suppress made with respect to such interceptions, and the number granted or denied;

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

(m) The information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year and not yet reported; and

(n) Other information required by the rules and regulations of the administrative office of the United States Courts.

(2) In March of each year the administrative director of the courts shall transmit to the legislature a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the administrative

director of the courts by the attorney general and prosecuting attorneys.

Sec. 803-48 Recovery of civil damages authorized. Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this part shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person:

(a) Actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation;

(b) Punitive damages; and

(c) A reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order shall constitute a complete defense to any civil action against an individual, but shall not constitute a defense to civil liability of the State.

Sec. 803-49 Severability. If any portion or subsection of this part or the application thereof to any person or circumstances is invalid, such invalidity shall not affect other sections or applications of the part which can be given effect without the

invalid section or application, and to this end the provisions of this part are declared to be severable."

SECTION 3. This Act shall take effect upon its approval and shall be effective for a period of six years.

APPENDIX II

TEXT OF THE FEDERAL WIRETAP STATUTE

CHAPTER 119—WIRE INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.

Historical Note

1968 Amendment. Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 212, added chapter 119 and items 2510-2520.

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any communication 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 furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

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

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

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

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

(6) "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;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; and.

"(d) [Function] It shall be the duty of the Commission to conduct a comprehensive study and review of the operation of the provisions of this title, in effect on the effective date of this section, to determine the effectiveness of such provisions during the six-year period immediately following the date of their enactment [June 19, 1968].

"(e) [Personnel; appointment; compensation and qualifications] (1) Subject to such rules and regulations as may be adopted by the Commission the Chairman shall have the power to—

"(A) appoint and fix the compensation of an Executive Director, and such additional staff personnel as he deems necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS-18 of the General Schedule under section 5332 of such title; and

"(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

"(2) In making appointments pursuant to paragraph (1) of this subsection, the Chairman shall include among his appointment individuals determined by the Chairman to be competent social scientists, lawyers, and law enforcement officers.

"(f) [Compensation, travel and other expenses] (1) A member of the Commission who is a Member of Congress shall serve without additional compensation, but shall be reimbursed for travel, subsistence, and other necessary expenses incurred in the performance of duties vested in the Commission.

"(2) A member of the Commission from private life shall receive $100 per diem when engaged in the actual performance of duties vested in the Commission, plus reimbursement for travel, subsistence, and other necessary expenses incurred in the performance of such duties.

"(g) [Cooperation of Federal and State agencies] Each department, agency, and instrumentality of the executive branch of the Government, including independent agencies, is authorized and directed to furnish to the Commission, upon request made by the Chairman, such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section. The Chairman is further authorized to call upon the departments, agencies, and other offices of the several States to furnish such statistical data, reports, and other information as the Commission deems necessary to carry out its functions under this section.

"(h) [Reports to President and Congress; termination date] The Commission shall make such interim reports as it deems advisable, and it shall make a final report of its findings and recommendations to the President of the United States and to the Congress within the one-year period following the effective date of this subsection. Sixty days after submission of its final report, the Commission shall cease to exist.

"(i) [Conflict of interest; exemption] (1) Except as provided in paragraph (2) of this subsection, any member of the Commission is exempted, with respect to his appointment, from the operation of sections 203, 205, 207, and 209 of title 18, United States Code.

"(2) The exemption granted by paragraph (1) of this subsection shall not extend—

"(A) to the receipt of payment of salary in connection with the appointee's Government service from any source other than the private employer of the appointee at the time of his appointment, or

"(B) during the period of such appointment, to the prosecution, by any person so appointed, of any claim against the Government involving any matter with which such person, during such period, is or was directly connected by reason of such appointment.

"(j) [Appropriations] There is authorized to be appropriated such sum as may be necessary to carry out the provisions of this section.

"(k) [Effective date] The foregoing provisions of this section shall take effect upon the expiration of the six-year period immediately following the date of the enactment of this Act [June 19, 1968]."

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

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

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 112.

Historical Note

References in Text. Section 153(h) of title 47 of the United States Code, referred to in par. (10), is section 153(h) of Title 47, Telegraphs, Telphones, and Radiotelegraphs.

Congressional Findings. Section 801 of Pub.L. 90-351 provided that:

"On the basis of its own investigations and of published studies, the Congress makes the following findings:

"(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

"(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

"(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

"(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."

National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. Section 804 of Pub.L. 90-351 provided that:

"(a) [Establishment] There is hereby established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (hereinafter in this section referred to as the 'Commission').

"(b) [Membership] The Commission shall be composed of fifteen members appointed as follows:

"(A) Four appointed by the President of the Senate from Members of the Senate;

"(B) Four appointed by the Speaker of the House of Representatives from Members of the House of Representatives; and

"(C) Seven appointed by the President of the United States from all segments of life in the United States, including lawyers, teachers, artists, businessmen, newspapermen, jurists, policemen, and community leaders, none of whom shall be officers of the executive branch of the Government.

"(c) [Chairman; vacancies] The President of the United States shall designate a Chairman from among the members of the Commission. Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

Library References

Telecommunications ⇐491 et seq.

C.J.S. Telegraphs, Telephones, Radio, and Television §§ 287, 288.

Notes of Decisions

Generally 2
Retroactive effect 1

1. Retroactive effect

This chapter applies only prospectively. U. S. v. American Radiator & Standard Sanitary Corp., D.C.Pa.1968, 288 F.Supp. 701.

2. Generally

This chapter is directed to reliability components of confession-exclusion rules, not to extrinsic policy components. U. S. v. Schipani, D.C.N.Y.1968, 289 F.Supp. 43.

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

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

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

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

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) 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 interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

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

(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection;

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) (a) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral 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.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral 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 or for the purpose of committing any other injurious act.

(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential

attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

Added Pub.L. 90–351, Title III, § 802, June 19, 1968, 82 Stat. 213.

Historical Note

References in Text. Chapter 5 of title 47 of the United States Code, referred to in par. (2) (b), is chapter 5 of Title 47, Telegraphs, Telephones, and Radiotelegraphs. Such chapter 5, set out as section 151 et seq. of Title 47, is the Communications Act of 1934.

Section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605), referred to in par. (3), is section 605 of Title 47, Telegraphs, Telephones, and Radiotelegraphs.

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Telecommunications ⟸491, 493, 494.

C.J.S. Telegraphs, Telephones, Radio, and Television §§ 122, 252, 287, 288.

Notes of Decisions

Crimes 3
Enforcement 2
Probable cause 1

---

1. Probable cause

General rule, under this chapter prohibiting unauthorized electronic surveillance, is that eavesdropping and wiretapping are permitted only with probable cause and a warrant. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L.Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

2. Enforcement

Without experience showing the contrary Supreme Court should not assume that this chapter prohibiting unauthorized electronic surveillance will be cavalierly disregarded or will not be enforced against transgressors. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L.Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

3. Crimes

Telephone subscriber is not authorized to use his telephone to commit a crime. State v. Holliday, Iowa 1969, 169 N.W.2d 768.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in 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 or oral communications;

(b) manufactures, assembles, possesses, or sells 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 or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) 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 or oral communications; or

(ii) 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 or oral communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier's business, or

(b) 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, to send through the mail, send or carry in 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 or oral communications.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 214.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Telecommunications ⇐191. C.J.S. Telegraphs, Telephones, Radio, and Television §§ 287, 288.

§ 2513. Confiscation of wire or oral communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 215.

Historical Note

References in Text. Title 19 of the United States Code, referred to in text, is Title 19, Customs Duties.

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Forfeitures ⇐3. C.J.S. Forfeitures § 3.

§ 2514. Immunity of witnesses

Whenever in the judgment of a United States attorney the testimony of any witness, or the production of books, papers, or other evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any violation of this chapter or any of the offenses enumerated in section 2516, or any conspiracy to violate this chapter or any of the offenses enumerated in section 2516 is necessary to the public interest, such United States attorney, upon the approval of the Attorney General, shall make application to the court that the witness shall be instructed to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him may tend to incriminate him or subject him to a penalty or forfeiture. No such witness shall be prosecuted or subjected to any penalty or forfeiture for or on account of any transaction, matter or thing concerning which he is compelled, after having claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except in a proceeding described in the next sentence) against him in any court. No witness shall be exempt under this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 216.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Criminal Law ⇐42. C.J.S. Criminal Law §§ 41, 46.

Notes of Decisions

1. Constitutionality

This section authorizing court to order witness to testify and providing that witness should not be excused on ground of self-incrimination and that he should be immune from prosecution as to anything concerning which he had been compelled to testify, as applied to witnesses before grand jury inquiring into matters involving interstate travel to promote riots, granted immunity coextensive with witnesses' privilege not to incriminate them-

selves, and was not unconstitutional. Carter v. U. S., C.A.Cal.1969, 417 F.2d 384.

This section authorizing court to order witness to testify and providing that witness should not be excused on ground of self-incrimination and that he should be immune from prosecution as to anything concerning which he had been compelled to testify does not unconstitutionally hamper states in prosecuting offenses that are contrary to their laws, thereby trenching upon reserved powers of the state. Id.

Grand jury witnesses had standing to question constitutionality of this section. Id.

Witnesses, who refused to answer questions before grand jury relating to matters involving interstate travel to organize, promote and encourage riots and to teach and demonstrate use and making of firearms and explosives on ground that answers might tend to incriminate them, had standing to challenge constitutionality of this section and section 2101 et seq. of this title, at hearing of government's motion for order granting immunity. In re Shead, D.C.Cal.1969, 302 F.Supp. 560, affirmed 417 F.2d 384.

2. Construction

This section did not limit immunity in criminal proceedings to testimony, as opposed to other evidence which may be compelled, and was sufficiently broad in its grant of immunity. In re Shead, D.C. Cal.1969, 302 F.Supp. 560, affirmed 417 F. 2d 384.

3. Application for order

In determining that in judgment of a United States attorney the testimony sought to be compelled before grand jury was necessary to public interest, court to which application for order to compel testimony was made did not have power to inquire into accuracy or merits of judgment as Congress had left judgment to executive discretion. In re Shead, D.C. Cal.1969, 302 F.Supp. 560, affirmed 417 F. 2d 384.

4. Self incrimination

Even if answering grand jury's questions concerning a trip to Canada would have incriminated witness in Canada, answers to questions directly relating to destruction of public service towers in Denver and the surrounding area and from which witness was granted complete immunity within the United States could not present a danger of incrimination in either the United States or Canada, so that witness' refusal to answer latter questions was clearly not justified, and she could properly be held in civil contempt. In re Parker, C.A.Colo.1969, 411 F.2d 1067.

Privilege against self-incrimination under U.S.C.A.Const. Amend. 5 provides no shelter for a person against incrimination in a foreign jurisdiction when provisions of this section granting immunity from both federal and state prosecution are applied. Id.

Since grand jury witness had specifically been granted immunity from both federal and state prosecution, and since any evidence, inculpatory or otherwise, related by witness during proceeding would be unavailable to the Canadian government in either an extradition proceeding in United States or in a criminal proceeding in Canada, witness was not justified in refusing to answer questions of grand jury on grounds that there was danger of incrimination in Canada. Id.

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication 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 the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 216.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Criminal Law ⇐394.3
Evidence ⇐154.

C.J.S. Criminal Law § 657(21) et seq.
C.J.S. Evidence § 187.

Notes of Decisions

Crimes 4
Disclosures within section 2
Evidence 3
Retroactive effect 1

1. Retroactive effect

This chapter relating to disclosure of contents of wire or oral communication which has been intercepted applies prospectively and did not preclude applicability of discovery provisions to tapes of conversations made prior to adoption of act. Philadelphia Housing Authority v. American Radiator & Standard Sanitary Corp., D.C.Pa.1968, 291 F.Supp. 247.

This section providing that any wire or oral communication could not be admitted in evidence if disclosure of information therein would be in violation of this chapter did not apply retroactively to authorize suppressing tape recordings of telephone conversations and meetings and evidence derived therefrom applicable to 17 corporate defendants charged with antitrust violations where the recordings were taken before effective date of this chapter. U. S. v. American Radiator & Standard Sanitary Corp., D.C.Pa.1968, 288 F.Supp. 701.

2. Disclosures within section

Defense counsel who would review tapes of conversations and would produce them pursuant to order of court could not be held to violate provisions of this chapter relating to disclosure of intercepted communications. Philadelphia Housing Authority v. American Radiator & Standard Sanitary Corp., D.C.Pa.1968, 291 F.Supp. 247.

3. Evidence

Where pen register was attached by telephone company to defendant's telephone line with knowledge and consent of recipient of threatening calls, evidence that calls were made from defendant's telephone to recipient's telephone did not violate this section prohibiting the unauthorized interception and divulgence of any telephone communication. State v. Holliday, Iowa 1969, 169 N.W.2d 768.

4. Crimes

Telephone subscriber is not authorized to use his telephone to commit a crime. State v. Holliday, Iowa 1969, 169 N.W.2d 768.

§ 2516. Authorization for interception of wire or oral communications

(1) The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal 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—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), or sections 2314 and 2315 (interstate transportation of stolen property);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or

(g) any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the ap-

plicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers 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 the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

Added Pub.L. 90–351, Title III, § 802, June 19, 1968, 82 Stat. 216.

Historical Note

References in Text. Sections 2274 through 2277 of title 42 of the United States Code, referred to in par. (1) (a), are sections 2274 through 2277 of Title 42, The Public Health and Welfare.

Sections 186 and 501(c) of title 29, United States Code, referred to in par. (1) (b), are sections 186 and 501(c), respectively, of Title 29, Labor.

Legislative History. For legislative history and purpose of Pub.L. 90–351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Searches and Seizures ⇐3.5.
Telecommunications ⇐493.

C.J.S. Searches and Seizures § 73 et seq.
C.J.S. Telegraphs, Telephones, Radio, and Television §§ 122, 287.

§ 2517. Authorization for disclosure and use of intercepted wire or oral communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may 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.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under

oath or affirmation in any criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding.

(4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 217.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Searches and Seizures ⇐3.5.
Telecommunications ⇐493.

C.J.S. Searches and Seizures § 73 et seq.
C.J.S. Telegraphs, Telephones, Radio, and Television §§ 122, 267.

Notes of Decisions

1. Generally

Divulgence at trial or to other government agents, of information obtained by prohibited electronic surveillance, is prohibited by this chapter. U. S. v. Schipani, D.C.N.Y.1968, 289 F.Supp. 43.

§ 2518. Procedure for interception of wire or oral communications

(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

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

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

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

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

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

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

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

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

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

(5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chap-

ter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, 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.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral 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 chapter to authorize such interception,

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire or oral 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 his 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 subsections (1) and (2) of section 2517 of this chapter 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 or oral communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter 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.

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

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7) (b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire or oral communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which

the interception was authorized or approved. This ten-day period may be waived by the judge if he 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.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

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

(iii) 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 chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify 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 thirty days after the date the order was entered and shall be diligently prosecuted.

Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 218.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90-351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Searches and Seizures ⇐3.5.
Telecommunications ⇐493.

C.J.S. Searches and Seizures § 73 et seq.
C.J.S. Telegraphs, Telephones, Radio, and Television §§ 122, 287.

Notes of Decisions

1. Prerequisites to issuance of warrant

Findings of fact prerequisite to issuance of investigative warrant under this chapter need not be set forth in warrant itself, especially where it appears from affidavit or other evidence submitted to issuing judge that such findings as are required thereby would clearly have been authorized. Cross v. State, Ga.1969, 171 S.E.2d 507.

2. Discovery and inspection

For purpose of resolving issue whether evidence against any defendant grew out of his illegally overheard conversations or conversations occurring on his premises, surveillance records as to which any defendant has standing to object should be turned over to him without first being submitted to trial judge for in camera examination as to relevancy. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U. S. 165, 22 L.Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

Government's representation that overheard product of electronic eavesdropping was not relevant to indictment did not afford defense to defendant's request for discovery concerning such eavesdropping, and court would not make determination of relevance in in camera inspection. U. S. v. McCarthy, D.C.N.Y.1968, 292 F.Supp. 937.

3. Suppression of evidence

Conversations overheard as result of unauthorized electronic surveillance are inadmissible in evidence against owner of premises whether or not he was present on the premises or party to the overheard conversation. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L. Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

This chapter renders any recordings obtained as result of wire-tapping without compliance with federal statute inadmissible in evidence irrespective of constitutionality of state wire-tapping statute Cross v. State, Ga.1969, 171 S.E.2d 507.

Where orders authorizing tapping of telephone lines failed to comply with requirements of this chapter because they failed to include provisions that orders should be executed as soon as practicable, failed to state whether interception of conversations should automatically terminate when described communication was first obtained, and that search should be conducted in such way as to minimize interception of communications not subject to seizure, and should terminate on attainment of authorized objective, recordings were inadmissible. Id.

4. Aggrieved persons

Under subsec. (10) (a) of this section prohibiting unauthorized electronic surveillance and providing that an aggrieved person may move to suppress the contents of a wire or oral communication illegally intercepted, phrase "aggrieved person" should be construed in accordance with existent standing rules. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L.Ed.2d 176, rehearing denied 89 S. Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

Unlawful wiretapping or eavesdropping, whether deliberate or negligent, can produce nothing usable against the defendant aggrieved by the invasion. Id.

§ 2519. Reports concerning intercepted wire or oral communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

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

(b) the kind of order or extension applied for;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

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

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

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

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

Added Pub.L. 90–351, Title III, § 802, June 19, 1968, 82 Stat. 222.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90–351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Searches and Seizures ⟸3.5.
Telecommunications ⟸493.

C.J.S. Searches and Seizures § 73 et seq.
C.J.S. Telegraphs, Telephones, Radio and Television §§ 122, 287.

§ 2520. Recovery of civil damages authorized

Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(b) punitive damages; and

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

A good faith reliance on a court order or on the provisions of section 2518(7) of this chapter shall constitute a complete defense to any civil or criminal action brought under this chapter.

Added Pub.L. 90–351, Title III, § 802, June 19, 1968, 82 Stat. 223.

Historical Note

Legislative History. For legislative history and purpose of Pub.L. 90–351, see 1968 U.S.Code Cong. and Adm.News, p. 2112.

Library References

Searches and Seizures ⟸8.

C.J.S. Searches and Seizures §§ 90-104.

Notes of Decisions

Enforcement 2
Probable cause 1

---

1. Probable cause

General rule, under this chapter prohibiting unauthorized electronic surveillance, is that eavesdropping and wiretapping are permitted only with probable cause and a warrant. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L.Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

2. Enforcement

Without experience showing the contrary Supreme Court should not assume that this chapter prohibiting unauthorized electronic surveillance will be cavalierly disregarded or will not be enforced against transgressors. Alderman v. U. S., Colo. & N.J.1969, 89 S.Ct. 961, 394 U.S. 165, 22 L.Ed.2d 176, rehearing denied 89 S.Ct. 1177, 394 U.S. 939, 22 L.Ed.2d 475.

APPENDIX III

STATE OF THE ART OF ELECTRONIC SURVEILLANCE

PURPOSE

The purpose of this appendix is to describe the state of the art of electronic surveillance. Technological advances in the field of electronics, especially the development of the transistor and the integrated circuit, have made possible a large array of new devices and techniques for electronic surveillance in recent years. These same advances have also improved the effectiveness of countermeasures against electronic surveillance.

KINDS OF ELECTRONIC SURVEILLANCE

In general, electronic surveillance can be divided into two classes: audio and non-audio.

Audio surveillance includes the interception of telephone conversations (wiretapping), and eavesdropping on conversations in otherwise private places by means of electronic devices (bugging).

Non-audio surveillance includes the interception of bulk data communications links, computer systems, visual sighting systems for

low light-level conditions, and electronic vehicle and cargo tracking systems. Non-audio surveillance will not be covered in this appendix.

AUDIO SURVEILLANCE

The division of audio surveillance into two types, wiretapping and bugging, is done to distinguish the kinds of conversations that are to be surveilled, i.e., telephonic and non-telephonic. In practice, there is an intermixture of techniques and devices used in audio surveillance. For example, radio transmitters used for bugging may also be used to transmit a tapped telephone conversation to a convenient listening or recording post. Similarly, telephone wires may be used to carry a conversation picked up by a hidden microphone "bug" to a remote listening post.

WIRETAPPING

The history of wiretapping predates the invention of the telephone. One of its earliest recorded uses occurred during the U.S. Civil War when intelligence agents of the opposing armies tapped telegraph lines to intercept messages about troop movements and battle plans.

Telephone wiretapping came into use soon after the invention of the telephone. Its practical value depends on several factors:

1. The kind of information contained in the telephone conversation;

2. The need of the wiretapper to gain this information;

3. The intelligibility of the intercepted conversation;

4. The security of the wiretap against detection; and

5. The convenience and cost of establishing and maintaining the wiretap.

It should be noted that the same factors apply to bugging. Because this appendix is meant to describe the state of the art of electronic surveillance, only the latter three factors will be discussed.

TELEPHONE SYSTEMS

Telephone conversations are carried from one telephone instrument to another over pairs of wires which are inter-connected by automatic switching equipment located in telephone company substations and central exchanges. The telephone system provides all the electrical power needed to operate the telephones as well as the various electronic signals which cause dial tones, ringing, and busy signals. Some of these features may be used to advantage in telephone surveillance

as well as in the detection of wiretaps and bugs.

WIRETAPS

When a listening device, such as a set of headphones, loudspeaker, or tape recorder, is connected to a pair of wires at some point between two telephone instruments, then the conversation can be intercepted. Two methods are used to connect the listening device to the telephone line. One method uses a wire coil to inductively couple* the audio signals on the line to the listening device. The other method uses a direct wire connection with electronic matching network.** Properly installed, neither method creates noises on the line or fluctuations in loudness that would alert users of the telephone to the existence of the tap. However, the direct wire equipment is much easier to attach and provides a more reliable and usable output signal

A magnetic field of varying intensity surrounds a wire through which a varying electrical current is flowing. The field is intensified or concentrated if the wire is wound in the form of a coil. If a second coil is placed close to the first, a proportional electrical current will flow through the second coil. This process is called induction.

**Electrical and electronic circuits exhibit certain electrical characteristics which can be measured. When two circuits are connected together, they should be as nearly alike as possible for maximum efficiency. The term impedence matching is used to describe the process of adding electronic components to a circuit to match its impedence to another. Impedence is the resistance to the flow of alternating current and results from the combined effect of resistance, inductance and capacitance.*

CONTINUED

2 OF 3

than the induction coil method. Electronic tests* of the telephone line by the telephone company are usually able to determine if foreign instruments are connected to the line. Similar checks by private countermeasure experts, without the cooperation of the telephone company, are less successful.

HARDWIRE TAPS THROUGH THE CENTRAL EXCHANGE

Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, certain government agencies may obtain court authorization to conduct wiretapping. In such circumstances, the telephone company makes the hardwire connection to the specified telephone line and provides a leased wire to the agency's listening post. If the equipment in the listening post is isolated electronically from the line in a proper manner, the tap cannot be detected. This is the preferred method of wiretapping because of its reliability, superior performance, good audio quality, and security from detection.

A number of tests may be made. A basic one is to measure the voltage on the line. When not in use the line will measure 48 volts. When the handset is lifted off-hook, the voltage will drop to between 6 and 12 volts. Another indication is current flow. When the telephone is in use, a current of 60 to 100 milliamperes will flow through the instrument. Devices such as infinity transmitters function as though the telephone is in use, thus their presence can be determined with simple instruments such as volt-ohm meter. A sophisticated system called domain reflectometry send pulses of energy down telephone wires; these pulses are reflected from electrical junctions along the wire back to the source. A wiretap will appear as a new junction. A good history of the system installation must be known and the test must be performed by skilled personnel to be effective.

OTHER HARDWIRE TAPS

Other hardwire taps can be made at any point between the telephone instrument and the nearest telephone exchange. These taps may be made on the premises of the telephone user, at a nearby utility pole terminal box, or, in the case of apartment and office buildings, in wire closets or terminal rooms. Because it may be inconvenient to establish a listening post at the location of the tap, means must be provided to carry the intercepted telephone conversation to a remote location. This may be done by wire or radio transmission.

WIRE TRANSMISSION OF TELEPHONE TAPS

A separate telephone line may be leased from the telephone company to carry the tapped conversation to a remote location. However, this would be less possible if the tap was not sanctioned by the court order. A device called a telephone slave can be used which permits a convenient wire connection to a tapped telephone line. In use, two wires from the slave are connected to a pair of wires from the phone to be tapped. Two other wires from the slave are connected to a second telephone line pair with a known number. When the number of this second telephone is dialed from any other telephone, the slave device automatically connects the two lines so that the caller can hear conversations on either line. The slave device, while providing a convenient way to transmit a tapped conversation to a remote location,

tends to be unreliable and sometimes will cause the wiretapper's line to be held in the open position causing a busy signal the next time an attempt is made to activate the slave unit.

RADIO TRANSMISSION OF TELEPHONE TAPS

The more usual way of carrying the tapped conversation to a remote location is with a radio transmitter. The transmitter may be connected to the telephone line inside the telephone instrument, between the instrument and a terminal box, or at a convenient terminal box. A popular radio tap transmitter, the telephone drop-in mouthpiece, is simply placed in the telephone handset after removal of the original mouthpiece unit. Its utility is limited by the fact that it can be readily detected by visual inspection.

Because most radio tap transmitters use conventional FM modulation,* they are easily detected by field strength meters** and

Radio frequencies range between one thousand oscillations per second (one kilohertz - formerly kilocycle) and 100 billion oscillations per second (100 gigahertz). Commercial FM radio frequencies range between 88 million oscillations per second (88 megahertz) and 108 million oscillations per second (108 megahertz). Radio transmitters send out electrical energy at a single set frequency. Audio signals which range from about 50 hertz to about 10 thousand hertz may be transmitted by using them to modulate the radio carrier frequency. In FM modulation the frequency of the carrier is varied slightly above and below its standard frequency to conform with the variations in the audio signal.

**An electronic radio field detection device that detects the presence of radio-frequency (r-f) energy.*

countermeasure receivers,* especially when they are located on the premises being tapped. To avoid such detection, and because of the nature of the devices and the limitation of their power sources, radio tap transmitters send signals over very short distances, usually no more than a few city blocks. A common practice is to connect the radio tap receiver to a voice-actuated tape recorder** located in the locked trunk of a car parked on the street close to the transmitter. This permits the signal to be received and recorded without the necessity of the eavesdropper being present.

An important accessory sometimes used in connection with wiretaps permits the eavesdropper to record the phone numbers that are dialed on the target telephone. These devices are known as dial impulse recorders (or pen registers) for the older dial system, and touch tone decoders for the new push button telephones. These moderately priced ($1,000-$2,000) instruments automatically count the dial impulses or decode the touch tones and provide the user with a direct read-out of the number being called.

Radio receivers which, unlike a standard radio receiver, have high sensitivity and selectivity over the large radio spectrum, are capable of different demodulation techniques, exhibit frequency stability and capability to acquire weak signals and demonstrate rejection of unwanted signals in adjacent frequency ranges.

**When an audio signal is received at the input terminals of a voice-actuated tape recorder, a switch activates the recorder. Thus, the tape supply and battery power are used only when a signal is being received.*

BUGGING

Audio surveillance of conversations in private places has been going on at least since mankind moved from caves to thatched huts. Thus the name "eavesdropping." The advent of the microphone or "bug" has permitted the eavesdropper greater flexibility and the security of not having to stand under the eaves of a house next to an open window.

The earliest and simplest form of bugging consists of a concealed microphone connected by wire to a listening device. While still used at the present time, the simple bug has been supplemented by more sophisticated devices. Some of these devices rely on a portion of the telephone system, others use radio transmitters or light beams to carry their signals.

WIRE BUGS

Bugs connected by wire to listening posts, while the earliest form of bugging, have benefited from recent technological advances. Progress in miniaturization has allowed better concealment of microphones. Increases in sensitivity aid in concealment as well as improve the intelligibility of the monitored conversation.

Wire bugging systems have advantages over other methods including durability, security, limitless operating life and low cost.

The usual wire bug will have one or more miniature microphones concealed in a target room and connected to a remote amplifier and listening device by fine, easily concealed wire or conductive paint. Specialized microphones such as spike* and crystal contact** types can be used to pick up room conversations on or through a wall or partition. Ordinary permanent magnet speakers found in most radio, television sets and stereo systems can be used as eavesdropping microphones. While intended to produce sound from electrical energy, permanent magnet speakers can also do the reverse since they are structurally similar to dynamic microphones.*** They may be connected to a listening post by wire or radio without impairing their function as speakers.

SHOTGUN AND PARABOLIC MICROPHONES

Shotgun and parabolic microphones can be used to retrieve normal conversations from distances as great as 300 feet under ideal conditions. Both are directional devices which tend to exclude all sounds other than those coming from the direction in which they are pointed.

A contact type microphone with a long needle-like extension used for listening through walls.

***A crystal microphone depends for its operation on the generation of an electrical charge by the deformation of a crystal by sound waves. A contact microphone is designed to be attached directly to the surface to be monitored, when the surface vibrates as a result of sound waves which hit it.*

****The movement of a small coil of wire near a permanent magnet will generate a small electrical current in the coil. If the coil is attached to a thin diaphram, sound waves which strike the diaphram will generate a current which is proportional to the sound. This is a dynamic or magnetic microphone.*

A shotgun microphone uses an arrangement of various length tubes to achieve its directional capability. The parabolic microphone uses a parabolic reflector of from one and a half to four feet in diameter to concentrate the received audio energy. Both devices have limited use because they are difficult to disguise and because of background interference from wind and ambient noises. Because of their limitations they are most useful at night in an open field or park where the target conversation is taking place in an extremely quiet environment.

TELEPHONE BUGS

The most widely publicized bug that uses the telephone system is the infinity transmitter or harmonica bug. Inexpensive versions of the infinity transmitter are marketed as burglar detectors and electronic baby sitters. This device is not a transmitter in the sense of a radio transmitter, but rather a tone controlled switch connected between a microphone concealed in a room and the telephone system. In operation, the eavesdropper dials the target telephone and, before it rings, sounds a predetermined note on a tone producing device. If sounded in time, the tone will switch on the room microphone and its associated amplifier while preventing the telephone from ringing. The name infinity transmitter derives from the claim by an early manufacturer that the device can be operated from an infinite distance, that is, from the most distant telephone able to call the target telephone. The name harmonica bug results from the early use of a

harmonica to sound the selected tone.

Widespread publicity about the infinity transmitter has created a popular belief that it is more useful for eavesdropping than the facts would indicate. There are a number of difficulties encountered in using the device:

1. Not all telephone systems are compatible with a particular device. In some systems the audio connection between two telephones is not completed at the same time as the ringing signal. In such a situation the telephone will ring and must be answered before the tone switch can be triggered, thus impairing the security of the device.

2. During the period when the device is in operation, the telephone system's sensing equipment indicates that the line is busy so all incoming calls will receive the normal busy signal. This may raise questions that will alert the target person that something is wrong with the line.

3. A voltage change on the line caused by activation of the infinity transmitter can easily be detected by a technician.

4. Audio sensing equipment attached to the line can detect the same signal being received by the eavesdropper.

5. A variable tone may be inserted on the line to trigger a suspected infinity transmitter. If one exists, its presence can be detected by the methods described above. To defend against this countermeasure, some newer, more expensive devices require multiple tones or time-spaced tones to trigger the device. However, multiple tone sweeping devices are being perfected in response to this development.

6. The eavesdropper must activate the device repeatedly, increasing the possibility of detection, because there is no way of knowing when valuable or interesting conversation is taking place.

LISTEN BACKS AND KEEP ALIVES

Like the infinity transmitter, these devices permit the use of the telephone system to eavesdrop on room conversations. Because they are not tone activated and do not use separate microphones and amplifiers, "listen backs" and "keep alives" are smaller, less expensive, and less likely to be detected by visual inspection than is the infinity transmitter.

These devices consist of simple, electrical modifications to the hookswitch* of the target telephone instrument which operate by keeping the line open and the telephone mouthpiece active after a call from the eavesdropper's telephone is completed and the target telephone headset is returned to its cradle. Until the eavesdropper hangs up his telephone, conversation close to the target instrument can be overheard. However, by design, the carbon microphone** in the mouthpiece of the telephone performs poorly in picking up sounds more than a few inches from the front of the mouthpiece. "Listen backs" and "keep alives" suffer from many of the same disadvantages as the infinity transmitters

---

The switch in a telephone instrument actuated by the hook or plunger on which the handset rests when not in use.

***The original microphone invented by Alexander Graham Bell in 1876 is durable, reliable, rugged, and resistant to changes in humidity and temperature. In operation, an electrical current is passed through carbon granules in the microphone behind a thin diaphram. As sound pressure varies the compression on the carbon granules, their electrical resistance varies proportionally.*

and are more difficult to install. In addition, the presence of such a device can be easily determined by following the same procedure as that used by the eavesdropper to activate the device.

ON-LINE MICROPHONES

Most telephone installations contain unused pairs of wires which can be used by an eavesdropper to carry an audio signal. An on-line microphone is a bug and associated amplifier which is connected to an unused telephone wire pair. It cannot be dialed or used from a remote telephone to eavesdrop. Its main advantage is that it relieves the eavesdropper of the need to install a separate line or use a radio transmitter within the target premises. Its disadvantage is that the audio signal can be detected on the line during debugging operations.

TELEPHONE MODIFICATION OR COMPROMISE

This eavesdropping technique, like the "keep alive", uses the mouthpiece of the target telephone to pick up room conversations by a modification of the hookswitch, at the same time allowing the telephone to be used normally. In operation, the signals are picked up as in a usual telephone tap. While the modifications to the hookswitch are relatively simple and inexpensive, a high degree of technical skill is required to prevent the alteration or disruption of the normal electrical status of the telephone line when it is not in use, so as to

prevent detection by the telephone company. In addition, multiple line instruments with rotary line selection switching,* as found in many offices, prevents the selection of a single line pair from outside the office, thus thwarting the purpose of the eavesdropper. Telephone compromising of this kind is most likely with single line instruments, or within a building or office system in the case of multiple line systems.

RADIO BUGS

The fictional secret agent's bug in the olive of a martini is a technical reality. Recent advances in miniaturization for computer, hearing aid, and aerospace applications have made possible extremely small devices. Further miniaturization is limited by battery technology.

Radio bugs, regardless of their size, consist of a microphone, amplifier and modulation circuitry, antenna, and power supply. The size of a radio bug generally determines the distance its signal can be transmitted, the period of time it can be in operation, and, inversely, its price. The decision as to what kind of bug will be used depends upon such factors as the degree of concealment necessary, the range of

**Automatic selection of a telephone line not in use, where several lines enter an office system. If a tap is placed on line one and it is in use, incoming calls routed to line two could not be monitored by the wiretapper.*

transmission needed for the signal to be received, and the availability of funds. An additional consideration is the ease with which the signal from the bug can be detected in a debugging sweep. Radio bugs may be classified according to size, means of concealment, kind of modulation used, frequency range used, and cost.

MINIATURE RADIO BUGS

The smallest bug generally available to law enforcement agencies in this country is about the size of an aspirin tablet. It includes battery and microphone and costs about $2,000.

A somewhat larger bug, about the size of three cubes of sugar, costs less than $50 and transmits up to 350 feet. However, bugs of this kind have poor reliability and lack frequency stability.*

Most radio bugs with good performance characteristics, including frequency stability, effective range of one quarter to one half mile, and operating periods of 48 to 60 hours, tend to be from one to three cubic inches in volume and cost about $500. Future advances in electronic technology including reduction in the size of crystal frequency

*Ability of a transmitter to maintain a set carrier frequency within narrow limits. Poor stability results in poor reception quality.

control devices* and battery size reduction may make possible smaller high performance bugs at moderate cost.

RADIO BUG APPLICATIONS

The smallest bugs are useful for quick installation. They are called drop-in or quick plant transmitters. Because of their small size they must be retrieved regularly for battery replacement.

Agent or body transmitters designed to be carried by an individual are generally larger, more powerful and better constructed than drop-in bugs. They are usually about the size of a cigarette package, including batteries, and usually have crystal controlled frequencies for good stability.

Small radio bugs are often supplied in concealment packages consisting of normal household or office fixtures. A common type is made to look like an electric socket or cube tap. Because such a device is able to use standard electrical power for its operation it is able to be permanently installed. Such devices normally transmit a

*The carrier wave of a transmitter is generated by an oscillator which is designed to cause an electrical current to vary at a set frequency. Simple oscillators use tuned circuits which most easily pass currents at, or close to, the set frequency. The values of the components making up the tuned circuit will vary with changing atmospheric conditions and with time, thus allowing the carrier frequency to change. A crystal oscillator will generate a current with a frequency maintained within a very narrow range. It is little affected by heat, moisture or age.

signal over a distance of 700 to 1,200 feet and cost less than $500.

MODULATION TECHNIQUES

Most radio bugs use normal frequency modulation (FM) techniques. Some of the least expensive devices, sold as wireless microphones, use either FM or amplitude modulation (AM).* More sophisticated methods are used in a few, more expensive bugs, for added security.

An attractive, non-standard method is sub-carrier modulation. In this method the audio signal picked up by the microphone is first modulated onto a very low frequency (VLF)** signal. This combined signal is then used to modulate a high frequency signal for transmission. The resulting signal is not able to be demodulated by a conventional radio receiver because of its complexity. In most circumstances no signal at all will be observed because the VLF sub-carrier frequency is far above the audible range. To gain added security, the eavesdropper may select a main carrier frequency that is the same as a commercial broadcast station. Now a standard receiver would play back the commercial broadcast without affecting the sub-carrier signal. This technique adds security to the bug.

The amplitude or size of current variations in a radio carrier are changed to conform with an audio signal. AM is used for standard radio broadcasting.

**The radio spectrum band from 10 kilohertz to 100 kilohertz. It is found just below the standard radio broadcast band.*

A special class of modulation is involved in a bugging device called a passive reflector. The bug consists of a small metallic capsule, about three-quarters of an inch in diameter with a wire antenna about nine inches long (more or less, depending on the frequency of the system). One end of the capsule is a very thin metallic diaphragm which vibrates in sympathy with room sounds. There are no batteries or other power sources needed. A high powered radio transmitter, located outside the target premises, beams its signal at the reflective diaphragm. The radio signal is modulated by the room audio present on the vibrating diaphragm. The modulated signal is radiated by the short antenna to a radio receiver for recovery of the audio. In 1952 a device of this kind was discovered imbedded in a carving of the Great Seal of the United States, a gift of the Soviet Union government hanging in the office of the American Ambassador in Moscow. The Russians operated their device in the frequency range between our commercial VHF and UHF television channels.

FREQUENCY RANGE

Inexpensive devices such as wireless microphones or wireless baby monitors, which can be used as radio bugs, use the standard AM or FM broadcast bands.* As a consequence they are easily detected while in

The standard AM band is from 540 kilohertz to 1,600 kilohertz. The standard FM band is from 88 megahertz to 108 megahertz.

operation. In general, professional radio bugs are designed to operate at other frequencies to avoid the possibility of accidental discovery when a standard radio receiver is used in the vicinity of the bug. Most often they are operated in the very high (VHF) or ultra high (UHF) frequency range.*

A valuable method for increasing security of radio bugs that use the standard broadcast bands is "snuggling." This method can be used regardless of power, method of modulation, or frequency selected, although it is most effective in the FM broadcast band. A frequency is selected for the bug that is very close to that of a nearby powerful radio station. Because standard FM receivers usually operate with automatic frequency control circuits (AFC)** they automatically select the stronger of two very close signals, thus preventing accidental discovery. The eavesdropper must use a receiver modified to permit the weaker signal from the bug to be received. The same is true for the debugger.

The VHF band is from 30 megahertz to 300 megahertz. The UHF band is from 300 megahertz to three gigahertz. From one gigahertz to 10 gigahertz radio frequencies are called microwaves.

***Some FM receivers used in component stereo systems have an AFC defeat switch for fine tuning purposes. However, many of these receivers will not have the selectivity necessary to hear a weak transmitter snuggled close to a powerful signal.*

One type of bug uses the very low frequency (VLF) range which is found below the commercial AM broadcast band. These devices, called carrier current transmitters, modulate an FM signal at very low frequency along electric power lines or telephone lines. Very little radio energy is radiated into space at such low frequencies, but such signals move readily along any wire path. The technique is used in many wireless intercom devices sold to homeowners and hobbyists and in a few type of bugs. An important advantage is that they cannot be detected by radio receivers in most situations. Instead, a VLF receiver must be connected to the power line with appropriate filters to exclude the electrical power from the receiver. One disadvantage is limited range, since the carrier current signal is blocked by the transformers used on power networks. Sometimes the power company will install bypasses on the transformers for its own carrier current signaling and switching purposes.

OPTICAL DIRECTIONAL SYSTEMS

A new development in eavesdropping technology uses directional beams of light energy. Small solid state devices called light emitting

diodes (LED)* are available which produce invisible infrared or visible light. An LED, coupled with a microphone, power supply, and modulator, can be used to transmit a signal to a sensitive optical receiver some distance away for retrieval of the audio signal. Properly installed, detection of such a device would be extremely difficult, except by physical inspection.

Another optical device has received wide publicity as a sinister new advance in eavesdropping. This is the coherent laser beam** which can be used to detect minute vibrations of a glass window pane caused by nearby room conversation. The vibrations cause detectable shifts in the laser beam's wave length. The beam reflects off the window pane to a receiving site where the wave shifts are demodulated to recover the room audio. There are two difficulties with the laser beam/window reflection technique. Because the necessary equipment costs from $10,000 to $50,000 it is not cost effective. More significant is the fact that window panes are caused to vibrate by all sounds present in the environment including traffic and construction noises. They are also made to vibrate by the wind and by building vibration due to

---

LED devices are commonly used in displays of numbers in pocket calculators and electronic wrist watches. The intensity of the light emitted would be varied in modulation.

**A tight, coherent beam of visible or invisible light that can be transmitted over great distances with a low degree of degradation due to beam spreading, as in a non-coherent light beam.*

machinery, air conditioners, fans, running water, and plumbing. Many of these vibrations are of much greater amplitude than those caused by room conversations. The retrieval of small audio vibrations from this maze of signals is neither reliable nor practical.

AUDIO SECURITY COUNTERMEASURES

Individual audio security countermeasures or methods for debugging were discussed above in connection with several devices. It should be understood that effective debugging requires highly trained technicians equipped with instruments costing several tens of thousands of dollars and consumes considerable time. Even then, no countermeasures expert can give assurance that no taps or bugs exist. While it is true that some devices can be detected with simple procedures and inexpensive equipment, proper installation of sophisticated taps and bugs makes debugging an imperfect art.

END