

Contents

Report of the Director	5
Reporting Requirements of the Statute	6
Regulations	6
Summary and Analysis of Reports by Judges	7
Authorized Lengths of Intercepts	7
Locations	8
Offenses	9
Summary and Analysis of Reports by Prosecuting Officials	10
Nature of Intercepts	10
Costs of Intercepts	10
Arrests and Convictions	10
Summary of Reports for Years Ending December 31, 1989 Through 1999	12
Supplementary Reports	12

Text Tables

Table 1	
Jurisdictions With Statutes Authorizing the Interception of Wire, Oral, or Electronic Communications	13
Table 2	
Intercept Orders Issued by Judges During Calendar Year 1999	14
Table 3	
Major Offenses for Which Court-Authorized Intercepts Were Granted	17
Table 4	
Summary of Interceptions of Wire, Oral, or Electronic Communications	21
Table 5	
Average Cost per Order	24
Table 6	
Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed	28
Table 7	
Authorized Intercepts Granted Pursuant to 18 U.S.C. 2519	32
Table 8	
Summary of Supplementary Reports for Intercepts Terminated in Calendar Years 1989 Through 1998	33
Table 9	
Arrests and Convictions Resulting From Intercepts Installed in Calendar Years 1989 Through 1999	38

Appendix Tables

Table A-1: United States District Courts
Report by Judges 40

Table A-2: United States District Courts
Supplementary Report by Prosecutors 86

Table B-1: State Courts
Report by Judges 104

Table B-2: State Courts
Supplementary Report by Prosecutors 216

Report of the Director of the Administrative Office of the United States Courts

on

Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications

The Omnibus Crime Control and Safe Streets Act of 1968 requires the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The statute requires that specific information be provided to the AO, including the offense(s) under investigation, the location of the intercept, the cost of the surveillance, and the number of arrests, trials, and convictions that directly result from the surveillance. This report covers intercepts concluded between January 1, 1999, and December 31, 1999, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

From 1998 to 1999, the total number of intercepts authorized by federal and state courts increased 2 percent to 1,350, reflecting continued growth in applications involving the surveillance of drug offense operations (up 2 percent). Following a decrease of one half of one percent in 1998, the number of applications for orders by federal authorities rose 6 percent in 1999. The number of applications reported by state prosecuting officials dropped 2 percent in 1999, with fewer jurisdictions providing reports than in 1998. The number of federal intercept applications authorized has grown over the last 10 years, increasing 94 percent from 1989 to 1999, while state applications have risen 65 percent since 1989. The number of intercepts employed in drug-related investigations also has experienced significant growth. Drug offenders were targeted in 978 of the interceptions concluded in 1999, compared to 471 in 1989, a 108% increase.

The appendix tables of this report list all intercepts reported by judges and prosecuting officials for 1999. Appendix Table A-1 shows reports filed by federal judges and federal prosecuting officials. Appendix Table B-1 presents the same information for state judges and state prosecuting officials. Appendix Tables A-2 and B-2 contain information from the supplementary reports submitted by prosecuting officials about additional arrests and trials in 1999 arising from intercepts initially reported in prior years.

Title 18 U.S.C. Section 2519(2) mandates the submission of wiretap reports no later than January 31 of each year. This office, as is customary, sends a letter to the appropriate officials every year reminding them of the statutory mandate. Nevertheless, each year reports are received after the deadline has passed. Information received after the deadline will be included in next year's *Wiretap Report*; the number of missing state and local prosecutors' reports was lower in 1999 compared to 1998. The AO is grateful for the cooperation and the prompt responses we received from many officials around the nation.

Leonidas Ralph Mecham
Director

April 2000

Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications

Reporting Requirements of the Statute

Each federal and state judge is required to file a written report with the Director of the Administrative Office of the United States Courts (AO) on each application for an order authorizing the interception of a wire, oral, or electronic communication (18 U.S.C. 2519(1)). This report is to be furnished within 30 days of the denial of the application or the expiration of the court order (after all extensions have expired). The report must include the name of the official who applied for the order, the offense under investigation, the type of interception device, the general location of the device, and the duration of the authorized intercept.

Prosecuting officials who applied for interception orders are required to submit reports to the AO each January on all orders that were terminated during the previous calendar year. These reports contain information related to the cost of the intercept, the number of days the intercept device was actually in operation, the total number of intercepts, and the number of incriminating intercepts recorded. Results such as arrests, trials, convictions, and the number of motions to suppress evidence related directly to the use of intercepts also are noted.

Neither the judges' reports nor the prosecuting officials' reports contain the names, addresses, or phone numbers of the parties investigated. The AO is **not** authorized to collect this information.

This report tabulates the number of applications for interceptions that were granted or denied, as reported by judges, as well as the number of authorizations for which interception devices were installed, as reported by prosecuting officials. No statistics are available on the number of devices installed for each authorized order.

No report to the AO is required when an order is issued with the consent of one of the principal parties to the communication. Examples of such situations include the use of a wire interception to investigate obscene phone calls; the interception of a communication to which a police officer or police informant is a party; the use of a body microphone; or the use of only a pen register (a mechanical device attached to a telephone line to record on paper tape all numbers dialed from that line).

Regulations

The Director of the AO is empowered to develop and revise the reporting regulations and reporting forms for collecting information on intercepts. Copies of the regulations, the reporting forms, and the federal wiretapping statute may be obtained by writing to the Administrative Office of the United States Courts, Statistics Division, Washington, D.C. 20544.

The Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any specially designated Deputy Assistant Attorney General in the Criminal Division of the Department of Justice may authorize an application to a federal judge for an order authorizing the interception of wire, oral, or electronic communications. On the state level, applications are made by a prosecuting attorney "if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction. . . ."

Many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries. Consequently, arrests, trials, and convictions resulting from these interceptions often do not occur within the same year as the

installation of the intercept device. Under 18 U.S.C. 2519(2), prosecuting officials must file supplementary reports on additional court or police activity that occurs as a result of intercepts reported in prior years. Appendix Tables A-2 and B-2 describe the additional activity reported by prosecuting officials in their supplementary reports.

Table 1 shows that 45 jurisdictions (the federal government, the District of Columbia, the Virgin Islands, and 42 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. During 1999, a total of 28 jurisdictions reported using at least one of these three types of surveillance as an investigative tool.

Summary and Analysis of Reports by Judges

Data on applications for wiretaps terminated during calendar year 1999 appear in Appendix Tables A-1 (federal) and B-1 (state). The reporting numbers used in the appendix tables are reference numbers assigned by the AO; these numbers do not correspond to the authorization or application numbers used by the reporting jurisdictions. The

same reference number is used for any supplemental information reported for a communications intercept in future volumes of the *Wiretap Report*.

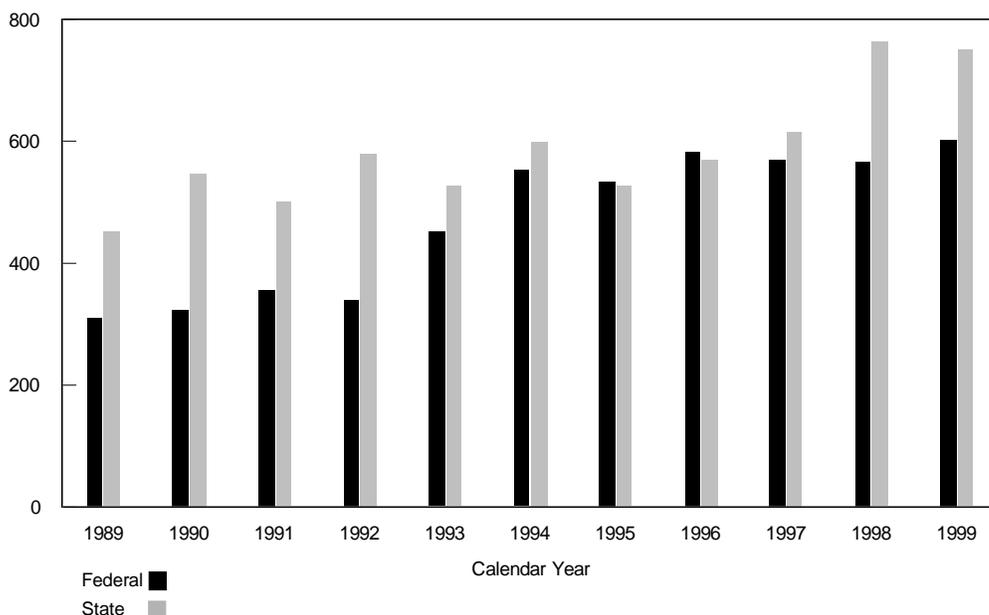
A total of 1,350 applications (an increase of 2 percent over 1998) were authorized in 1999, including 601 submitted to federal judges and 749 to state judges. Judges approved all applications. The number of applications approved by federal judges in 1999 increased 6 percent, while approvals by state judges fell 2 percent below the previous year's total. Wiretap applications in New York (343 applications), California (76 applications), New Jersey (71 applications), Pennsylvania (69 applications), and Illinois (50 applications) accounted for 81 percent of all authorizations approved by state judges.

Authorized Length of Intercepts

Table 2 presents the number of intercept orders issued in each jurisdiction that provided reports, the number of amended intercept orders issued, the number of extensions granted, the average length of the original authorizations and their extensions, the total number of days the

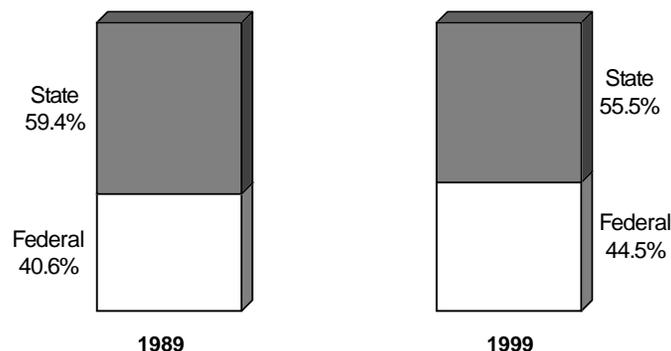
Federal and State Wiretap Authorizations

Number of authorizations



Federal and State Wiretap Authorizations

Percent of Total Authorizations



intercepts actually were in operation, and the nature of the location where each interception of communications occurred. Most state laws limit the period of surveillance under an original order to 30 days. This period, however, can be lengthened by one or more extensions if the authorizing judge determines that additional time for surveillance is warranted.

During 1999, the average length of an original authorization was 27 days, down from 28 days in 1998. A total of 1,367 extensions were requested and authorized in 1999 (an increase of 17 percent). The average length of an extension was 29 days, up from 27 days in 1998. The longest federal intercept occurred in the Western District of Texas, where the original 30-day order was extended nine times to complete a 289-day wiretap used in a narcotics investigation. Among state wiretaps terminating during 1999, the longest was used in a racketeering investigation in New York County, New York; this wiretap required a 30-day order to be extended 16 times to keep the intercept in operation 510 days. In contrast, 19 federal intercepts and 77 state intercepts each were in operation for less than a week.

Locations

The most common specific location for the placement of wiretaps in 1999 was a “single-family dwelling,” a type of location that includes houses, rowhouses, townhouses, and duplexes.

Table 2 shows that in 1999 a total of 18 percent (248 wiretaps) of all intercept devices were authorized for single-family dwellings; 7 percent (92 wiretaps) were authorized for apartments; and 4 percent (59 wiretaps) were authorized for business establishments such as restaurants and hotels.

Forty-nine percent of intercept applications (663 applications) specified “other” locations. Applications specifying other locations, which include electronic wiretaps such as mobile telephones, electronic pagers, and cellular telephones, have continued to increase in recent years with the proliferation of these types of communication devices. Combinations of locations were cited in 269 federal and state applications (20 percent of the total) in 1999.

Since the enactment of the Electronic Communications Privacy Act of 1986, a specific location need not be cited in a federal application if the application contains a statement explaining why such specification is not practical or shows “a purpose, on the part of that person (under investigation), to thwart interception by changing facilities” (see 18 U.S.C. 2518 (11)). In these cases, prosecutors use “roving” wiretaps to target a specific person rather than a specific telephone or location. The Intelligence Authorization Act of 1999, enacted on October 20, 1998, amended 18 U.S.C. 2518 (11)(b) so that a specific facility need not be cited “if there is probable cause to believe

that actions by the person under investigation could have the effect of thwarting interception from a specified facility.” The amendment also specifies that “the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.”

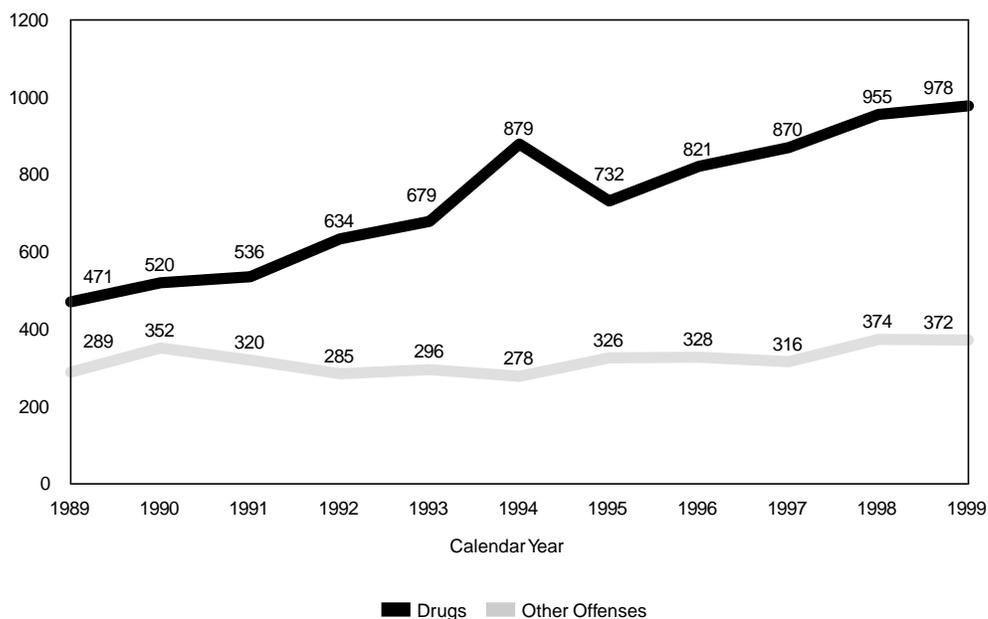
For the 1999 report, 94 wiretaps were implemented for which the authorizations indicated roving wiretaps were involved, either as the only location category reported (18 applications) or in combination with one or more other locations (76 applications). This year’s total was more than twice that for roving wiretaps reported for 1998, which is consistent with the fact that 1999 was the first full year of reporting since the enactment of the Intelligence Authorization Act of 1999. Federal authorities reported that they employed roving wiretaps for eight investigations; six were employed in drug offense investigations, one in a murder investigation, and one in a firearms investigation. On the state level, 86 roving wiretaps were reported; 52 percent (45 applications) were used in racketeering investigations, 31 percent (27 applications) in drug offense investigations,

and the remainder (14 applications) in investigations of other offenses. Roving wiretaps authorized in New York County, New York, accounted for 50 percent of all roving wiretaps reported in 1999; 47 applications in New York County, New York, indicated that roving wiretaps were employed, with the majority (43 applications) used in racketeering investigations.

Offenses

Violations of drug laws and racketeering laws remain the two most prevalent types of offenses investigated through communications intercepts. Homicide/assault was the third most frequently noted offense category cited on wiretap orders, and gambling offenses were the fourth most frequently cited offense category reported. Table 3 indicates that 72 percent of all applications for intercepts (978 cases) authorized in 1999 cited drug offenses as the most serious offense under investigation. Many applications for court orders indicated that several criminal offenses were under investigation, but Table 3 includes only the most serious criminal offense named in an application. The use of federal intercepts to conduct drug investigations was most common in the Central

Drugs as the Major Offense



District of California (38 applications) and the Southern District of Florida (34 applications). On the state level, the New York City Special Narcotics Bureau obtained authorizations for 135 drug-related intercepts, which accounted for the highest percentage (28 percent) of all drug-related intercepts reported by state or local jurisdictions in 1999. Nationwide, racketeering (139 orders), homicide/assault (62 orders), and gambling (60 orders) were specified in 10 percent, 5 percent, and 4 percent of authorizations, respectively, as the most serious offense under investigation.

Summary and Analysis of Reports by Prosecuting Officials

In accordance with 18 U.S.C. 2519(2), prosecuting officials must submit reports to the AO no later than January 31 of each year for intercepts terminated during the previous calendar year. Appendix Tables A-1 and B-1 contain information from all prosecutors' reports submitted for 1999. Judges submitted 42 reports for which the AO received no corresponding reports from prosecuting officials. For these authorizations, the entry "NP" (no prosecutor's report) appears in the appendix tables. Some of the prosecutors' reports may have been received too late to include in this report, and some prosecutors delayed filing reports to avoid jeopardizing ongoing investigations. Information received after the deadline will be included in next year's *Wiretap Report*.

Nature of Intercepts

Of the 1,350 communication interceptions authorized in 1999, intercept devices were installed in conjunction with a total of 1,277 orders. Table 4 presents information on the average number of intercepts per order, the number of persons whose communications were intercepted, the total number of communications intercepted, and the number of incriminating intercepts. Wiretaps varied extensively with respect to the above characteristics.

The average number of interceptions per day reported by all jurisdictions in 1999 ranged from less than 1 to nearly 500. The most active federal intercept occurred in the Southern District of New York, where a 90-day fraud investigation installa-

tion involved more than 1,790 agent workdays and resulted in an average of 490 interceptions per day. For state authorizations, the most active investigation was a 14-day drug offense operation in Oklahoma County, Oklahoma, that produced an average of 296 intercepts per day. Nationwide, in 1999 the average number of persons whose communications were intercepted per order in which intercepts were installed was 195. The average number of communications intercepted was 1,921 per wiretap; an average of 390 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order increased from 19 percent of interceptions in 1998 to 20 percent in 1999.

Table 6 presents the type of surveillance device used for each intercept installed. The most common method of surveillance reported was the electronic wiretap, which includes devices such as digital display pagers, voice pagers, cellular phones, and electronic mail. Electronic wiretaps accounted for 53 percent (676 cases) of intercepts installed in 1999. Telephone wiretaps, which were the most common type of wiretap prior to 1998, constituted 31 percent (399 cases) of intercept devices installed. Microphones were used in 5 percent of intercepts (58 cases). A combination of devices was used in 11 percent of intercepts (144 cases).

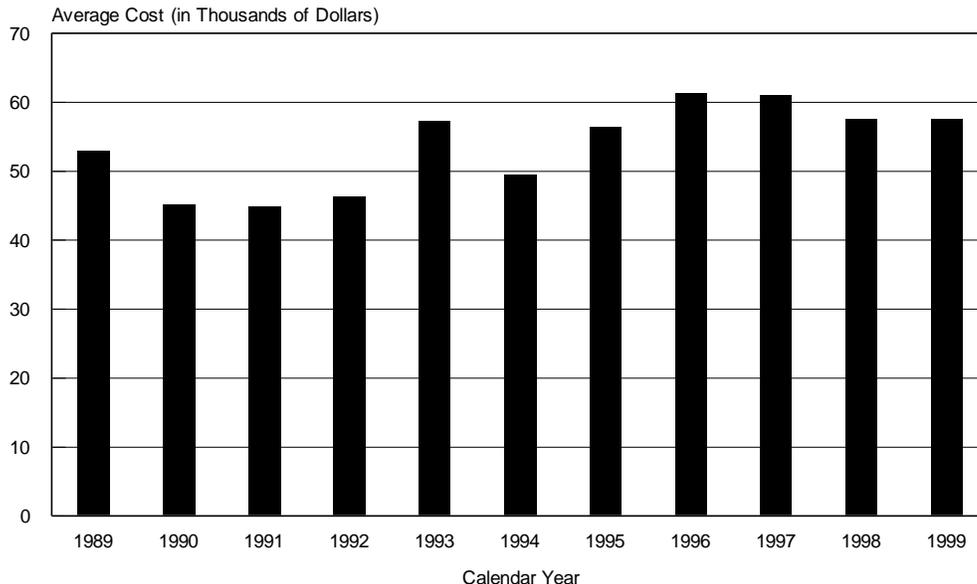
Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 1999. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,232 authorizations for which reports included cost data. The average cost of intercept devices installed in 1999 was \$57,511, essentially the same as in 1998 (down 0.3 percent). For federal wiretaps for which expenses were reported in 1999, the average cost was \$73,616, a 0.3 percent increase from the average cost in 1998. The average cost of a state wiretap fell 2 percent to \$43,231 in 1999. For additional information, see Appendix Tables A-1 (federal) & B-1 (state).

Arrests and Convictions

Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. The Southern District of

Average Cost of Wiretaps



Florida reported a federal telephone wiretap that led to the arrest of 26 persons and 23 subsequent convictions, and noted that this wiretap “was crucial to identifying the scope and participants of organizations, as well as the level of corruption.” Reporting officials describing a federal wiretap in the Middle District of Florida in use for 30 days in a drug conspiracy investigation stated that this intercept, which targeted a cocaine supply source, provided significant incriminating evidence and identified co-conspirators. In the District of New Jersey, a telephone wiretap in use for 60 days in a racketeering investigation led to the execution of search warrants resulting in the seizure of stolen property, expired food products, and other contraband. On the state level, the Berks County District Attorney’s office in Pennsylvania reported that a 44-day wiretap approved as part of a corruption investigation resulted in the arrest of 16 persons, 12 of whom were convicted, and noted that the interceptions were instrumental in obtaining convictions and “clearly established the organization, its structure, the players, and their roles. In addition, the interceptions strengthened the case so much that the twelve convictions were

obtained through guilty pleas.” The State Attorney’s office in Suffolk County, Massachusetts, reported that a wiretap in use for 57 days in a narcotics investigation resulted in 19 arrests and 10 subsequent convictions, and stated that without the wiretap evidence, “three separate organizations would still be actively dealing drugs.” In Middlesex County, New Jersey, a 15-day telephone wiretap used in a gambling investigation resulted in the seizure of gambling records and approximately \$45,000, and led to the arrest of 7 persons.

Table 6 presents the numbers of persons arrested and convicted as a result of interceptions reported as terminated in 1999. As of December 31, 1999, a total of 4,372 persons had been arrested based on interceptions of wire, oral, or electronic communications, 15 percent (654 persons) of whom were convicted (a decrease from the 1998 conviction rate of 26 percent, returning to a percentage rate closer to the 1997 conviction rate of 18 percent). Federal wiretaps were responsible for the most arrests (66 percent) and convictions (55 percent) during 1999. A wiretap in the Western District of New York resulted in the most arrests of any intercept in 1999. This wiretap,

which was the lead wiretap of three used in a narcotics investigation, led to the arrest of 83 persons. A wiretap in the Southern District of Florida produced the most convictions of any wiretap when an intercept used in a drug investigation resulted in the conviction of 23 of the 26 persons arrested. Among state intercepts, the wiretap producing the most arrests took place in Middlesex County, New Jersey, where an intercept conducted as part of a drug investigation resulted in the arrests of 72 persons. Two jurisdictions reported the largest number of convictions arising from state wiretaps (21 convictions each). In Suffolk County, New York, one intercept used in a drug investigation led to the conviction of 21 of the 33 persons arrested; in Kings County, New York, an intercept used in an investigation of assault, robbery, and conspiracy resulted in the conviction of 21 of the 28 persons arrested. Because criminal cases involving the use of electronic surveillance may still be under active investigation, the results of many of the intercepts concluded in 1999 may not have been reported. Prosecutors will report the costs, arrests, trials, motions to suppress evidence, and convictions related directly to these intercepts in future supplementary reports, which will be noted in Appendix Tables A-2 or B-2 of subsequent volumes of the *Wiretap Report*.

Summary of Reports for Years Ending December 31, 1989 Through 1999

Table 7 provides information on intercepts reported each year from 1989 to 1999. The table specifies the number of intercept applications requested, denied, authorized, and installed; the number of extensions granted; the average length

of original orders and extensions; the locations of intercepts; the major offenses investigated; average costs; and the average number of persons intercepted, communications intercepted, and incriminating intercepts. From 1989 to 1999, the number of intercept applications authorized increased 77 percent. The majority of wiretaps involved drug-related investigations, ranging from 62 percent of all applications authorized in 1989 to 72 percent in 1999.

Supplementary Reports

Under 18 U.S.C. 2519(2), prosecuting officials must file supplementary reports on additional court or police activity occurring as a result of intercepts reported in prior years. Because many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries, supplementary reports are necessary to fulfill reporting requirements. Arrests, trials, and convictions resulting from these interceptions often do not occur within the same year in which the intercept was first reported. Appendix Tables A-2 and B-2 provide detailed data from all supplementary reports submitted.

During 1999, a total of 2,076 arrests, 1,996 convictions, and additional costs of \$5,262,325 resulted from wiretaps completed in previous years. Table 8 summarizes additional prosecution activity by jurisdiction for intercepts terminated in the years noted. Most of the additional activity reported in 1999 involved wiretaps terminated in 1998. Intercepts concluded in 1998 led to 61 percent of arrests, 61 percent of convictions, and 74 percent of expenditures reported in 1999 for wiretaps terminated in prior years. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1989 through 1999.