Contents

Text Tables

Appendix Tables

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, 2002, and December 31, 2002, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 1,358 intercepts authorized by federal and state courts were completed in 2002, a drop of 9 percent compared to the number terminated in 2001. The number of applications for orders by federal authorities rose 2 percent to 497. Following an increase of 41 percent in 2001, the number of applications reported by state prosecuting officials dropped 14 percent in 2002. The average number of persons whose communications were intercepted increased 7 percent. The number of communications intercepted per order was 9 percent higher, and the number of incriminating communications reported per wiretap was 21 percent higher.

Public Law 106-197 amended 18 U.S.C. 2519(2)(b) to require that reporting should reflect the number of wiretap applications granted for which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. Encryption was reported to have been encountered in 16 wiretaps terminated in 2002 and in 18 wiretaps terminated in calendar year 2001 or earlier but reported for the first time in 2002; however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted.

The appendix tables of this report list all intercepts reported by judges and prosecuting officials for 2002. 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 2002 arising from intercepts initially reported in prior years.

Title 18 U.S.C. Section 2519(2) provides that prosecutors must submit wiretap reports to the AO 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, and the filing of some reports may be delayed to avoid jeopardizing ongoing investigations. The number of missing state and local prosecutors' reports was higher in 2002 compared to 2001. Information received after the deadline will be included in next year's *Wiretap Report*. The AO is grateful for the cooperation and the prompt response we received from many officials around the nation.

Leonidas Ralph Mecham
Director

April 2003

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 each 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. This report does not include interceptions regulated by the Foreign Intelligence Surveillance Act of 1978 (FISA).

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, or the use of a body microphone. Also, no report to the AO is required for the use of a pen register (a device attached to a telephone line that records or decodes impulses identifying the numbers dialed from that line) unless the pen register is used in conjunction with any wiretap devices whose use must be reported. Pursuant to 18 U.S.C. 3126, the U.S. Department of Justice collects and reports data on pen registers and trap and trace devices.

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."

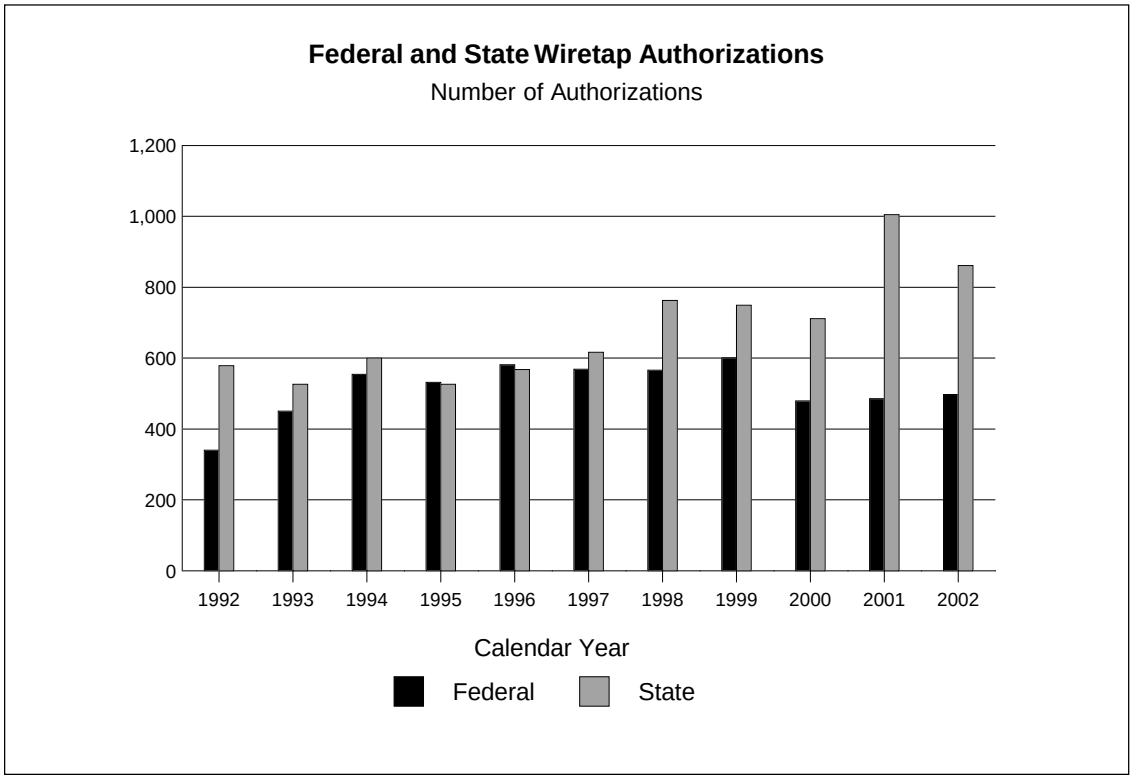
Many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries. Consequently, arrests, trials, and convictions resulting from these interceptions often do not occur within the same year as the installation of the intercept device. Under 18 U.S.C. 2519(2), 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 47 jurisdictions (the federal government, the District of Columbia, the Virgin Islands, and 44 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. During 2002, a total of 20 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 2002 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 reporting number is used for any supplemental information reported for a communications intercept in future volumes of the *Wiretap Report*.

After increasing 25 percent in 2001, the number of wiretaps reported decreased 9 percent in 2002. A total of 1,358 applications were authorized in 2002, including 497 submitted to federal judges and 861 to state judges. One application was denied. Compared to the number approved during 2001, the number of applications approved by federal judges in 2002 increased 2 percent, and the number of applications approved by state judges dropped 14 percent. Wiretap applications in New York (404 applications), California (143 applications), New Jersey (81 applications), Pennsylvania (79 applications), Maryland (54 applications), Florida (37 applications), and Illinois (25 applications) accounted for 96 percent of all authorizations approved by state judges. The number of states reporting wiretap activity was lower than the number for last year (19 states in 2002 compared to 24 in 2001), and reports were received from 80 separate state



jurisdictions in 2002, 20 fewer than the number of state jurisdictions that reported wiretaps in 2001.

Authorized Lengths 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 lengths of the original authorizations and their extensions, the total number of days the 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 2002, the average length of an original authorization was 29 days, up from 27 days in 2001. A total of 889 extensions were requested and authorized in 2002 (a decrease of 12 percent). The average length of an extension was 29 days, the same as in 2001. The longest federal intercept occurred in the District of Nevada, where an original 30-day order was extended 11 times to complete a 360-day wiretap used in a racketeering investigation. Among state wiretaps terminating during 2002, the longest was used in a narcotics investigation conducted by the New York State Organized Crime Task Force; this wiretap required a 30-day order to be extended 28 times to keep the intercept in operation 830 days. In contrast, 18 federal intercepts and 53 state intercepts each were in operation for less than a week.

Locations

The most common location specified in wiretap applications authorized in 2002 was "portable device, carried by/on individual," a category included for the first time in the *2000 Wiretap Report*. This category was added because wiretaps authorized for devices such as portable digital pagers and cellular telephones did not readily fit into the location categories provided prior to 2000. Table 2 shows that in 2002, a total of 77 percent (1,046 wiretaps) of all intercepts authorized were for portable devices such as these, which are not limited to fixed locations. This is an increase of 9 points over the percentage in 2001, when 68 percent of all intercepts involved portable devices.

The next most common specific location for the placement of wiretaps in 2002 was a "personal residence," a type of location that includes single-family houses, as well as row houses, apartments, and other multi-family dwellings. Table 2 shows that in 2002 a total of 11 percent (154 wiretaps) of all intercept devices were authorized for personal residences. Three percent (37 wiretaps) were authorized for business establishments such as offices, restaurants, and hotels. Combinations of locations were cited in 85 federal and state applications (6 percent of the total) in 2002. Finally, 2 percent (27 wiretaps) were authorized for "other" locations, which included such places as prisons, pay telephones in public areas, and motor vehicles.

Since the enactment of the Electronic Communications Privacy Act of 1986, a specific location need not be cited 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 2002, authorizations for nine wiretaps indicated approval with a relaxed specification order, meaning they were considered roving wiretaps. Federal authorities reported that roving wiretaps were approved for three investigations, with two authorized for use in racketeering investigations, and one for use in a drug offense

investigation. On the state level, six roving wiretaps were reported; five applications were authorized for use in drug offense investigations, and one for use in a robbery investigation.

Offenses

Violations of drug laws and gambling laws were the two most prevalent types of offenses investigated through communications intercepts. Racketeering was the third most frequently noted offense category cited on wiretap orders, and homicide/assault was the fourth most frequently cited offense category reported. Table 3 indicates that 77 percent of all applications for intercepts (1,052 wiretaps) authorized in 2002 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 Southern District of New York (45 applications), the Northern District of Illinois (35 applications), and the Central District of California (30 applications). On the state level, the New York City Special Narcotics Bureau obtained authorizations for 163 drug-related intercepts, which accounted for the largest percentage (25 percent) of all drug-related intercepts reported by state or local jurisdictions in 2002. Nationwide, gambling (82 orders), racketeering (72 orders), and homicide/assault (58 orders) were specified in 6 percent, 5 percent, and 4 percent of authorizations, respectively, as the most serious offense under investigation.

Summary and Analysis of Reports by Prosecuting Officials

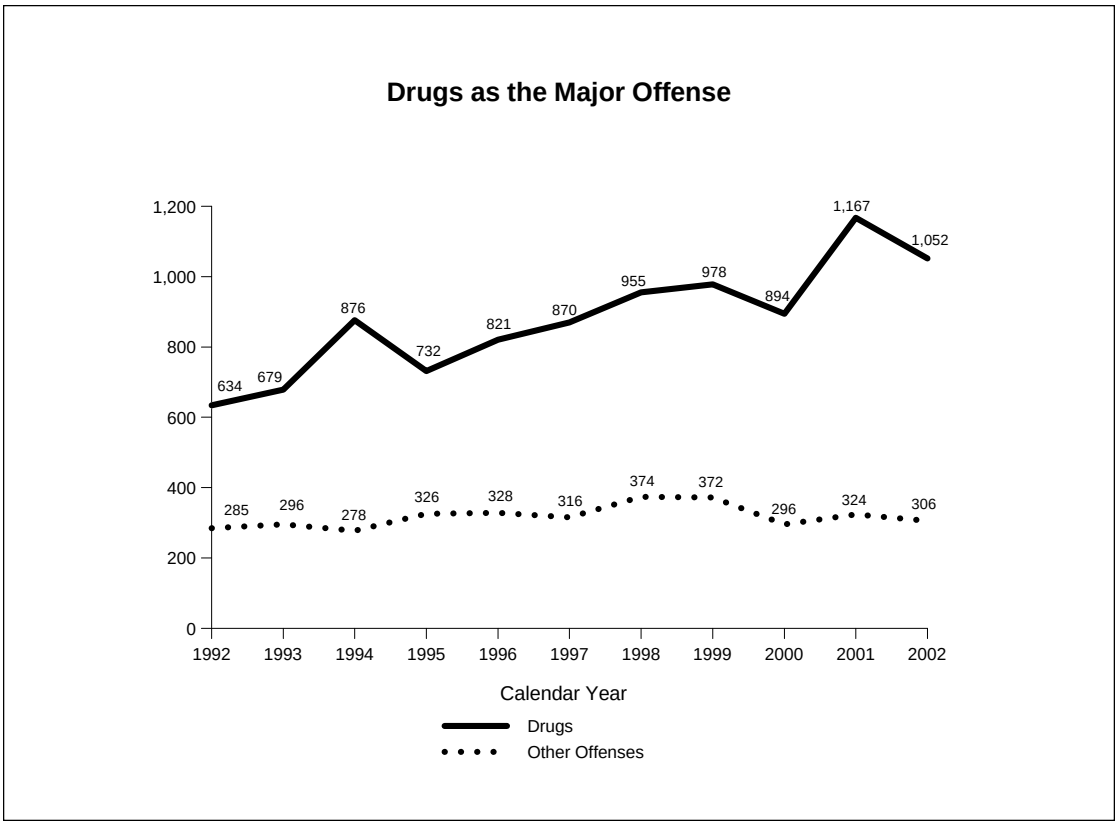
In accordance with 18 U.S.C. 2519(2), prosecuting officials must submit reports to the AO no later than January 31 of each year for intercepts terminated during the previous calendar year. Appendix Tables A-1 and B-1 contain information from all prosecutors' reports submitted for 2002. Judges submitted 58 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 1,358 communication interceptions authorized in 2002, intercept devices were installed in conjunction with a total of 1,273 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.

In 2002, installed wiretaps were in operation an average of 39 days, a 3 percent increase from the average number of days wiretaps were in operation in 2001. The average number of intercepts per day reported by jurisdictions in 2002 ranged from less than 1 to over 650. The most active federal intercept occurred in the Central District of California, where a 30-day narcotics conspiracy investigation involved cellular telephone intercepts and resulted in an average of 677 interceptions per day. For state authorizations, the most active investigation was a 60-day narcotics investigation in the Fourth Judicial Circuit (Duval County), Florida, that produced an average of 342 intercepts per day. Nationwide, in 2002 the average number of persons whose communications were intercepted per order in which intercepts were installed was 92, and the average number of communications intercepted was 1,708 per wiretap. An average of 403 intercepts per installed wiretap produced incriminating evidence, and the average percentage of incriminating intercepts per order rose from 21 percent of interceptions in 2001 to 24 percent in 2002.

The three major categories of surveillance are wire communications, oral communications, and electronic communications. In the early years of wiretap reporting, nearly all intercepts involved telephone (wire) surveillance, primarily communications made via conventional telephone lines; the remainder involved microphone (oral)



surveillance or a combination of wire and oral interception. With the passage of the Electronic Communications Privacy Act of 1986, a third category was added for the reporting of electronic communications, which most commonly involve digital-display paging devices or fax machines, but also may include some computer transmissions. The *1988 Wiretap Report* was the first annual report to include electronic communications as a category of surveillance.

Table 6 presents the type of surveillance method used for each intercept installed. The most common method of surveillance reported was "phone wire communication," which includes all telephones (landline, cellular, cordless, and mobile). Telephone wiretaps accounted for 88 percent (1,124 cases) of intercepts installed in 2002. Of those, 971 wiretaps involved cellular/mobile telephones, either as the only type of device under surveillance (922 cases) or in combination with standard telephones (49 cases).

The next most common method of surveillance reported was the electronic wiretap, which includes devices such as digital display pagers, voice pagers, fax machines, and transmissions via computer such as electronic mail. Electronic wiretaps accounted for 5 percent (59 cases) of intercepts installed in 2002; 86 percent of these (51 cases) involved electronic pagers. Microphones were used in 3 percent of intercepts (35 cases). A combination of surveillance methods was used in 4 percent of intercepts (55 cases); of these combination intercepts, 71 percent (39 cases) included a mobile/cellular telephone as one of the devices monitored.

Public Law 106-197 amended 18 U.S.C. 2519(2)(b) in 2001 to require that reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2002, no federal wiretap reports indicated that encryption was encountered. State and local jurisdictions reported that encryption was encountered in 16 wiretaps terminated in 2002; however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted. In addition, state and local jurisdictions reported that encryption was encountered in 18 wiretaps that were terminated in calendar year 2001 or earlier, but were reported for the first time in 2002; in none of these cases did encryption

prevent access to the plain text of communications intercepted.

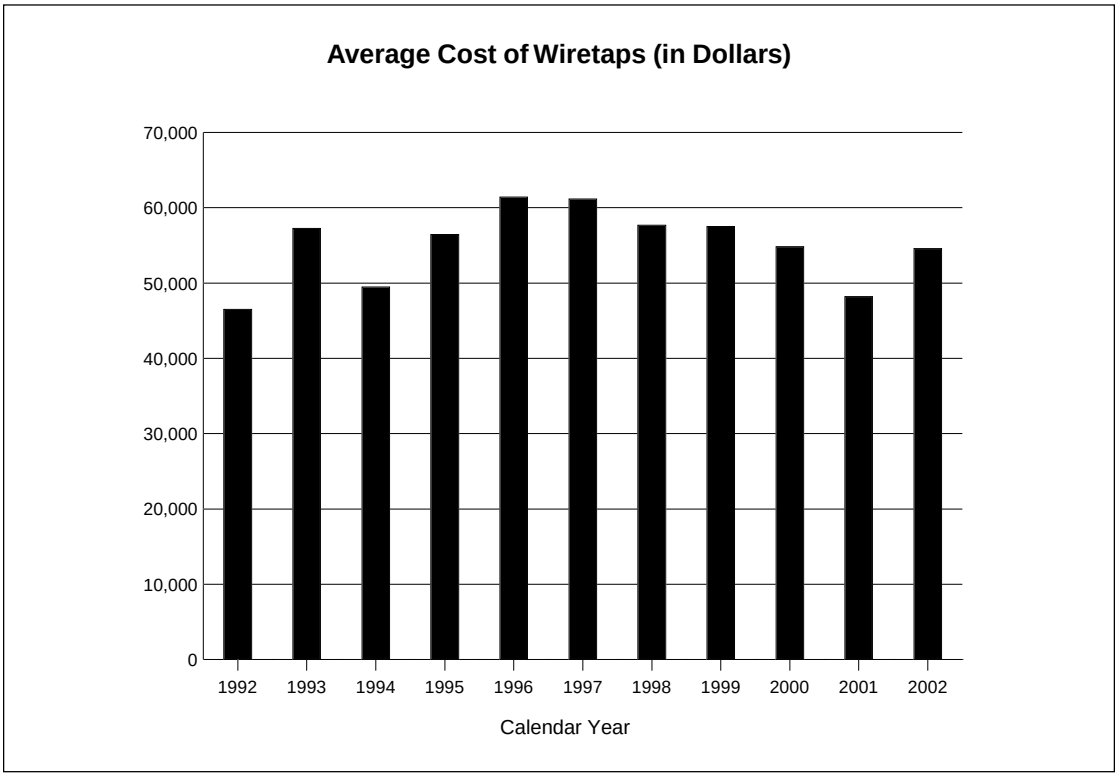
Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 2002. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,193 authorizations for which reports included cost data. The average cost of intercept devices installed in 2002 was $54,586, up 13 percent from the average cost in 2001. For federal wiretaps for which expenses were reported in 2002, the average cost was $75,659, a 2 percent increase above the average cost in 2001. The average cost of a state wiretap rose 19 percent to $40,101 in 2002. For additional information, see Appendix Tables A-1 (federal) and B-1 (state).

Arrests and Convictions

Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. The Central District of California reported a federal wiretap involving cellular telephone surveillance in a narcotics conspiracy investigation that led to 15 arrests and 1 conviction; in addition, the reporting officials noted that this wiretap "resulted in the seizure of 71.5 pounds of methamphetamine, 230 gallons of methamphetamine solution, 110 gallons of pseudo-ephedrine; 2 million pseudo-ephedrine tablets, 4 vehicles, 4 weapons, and $74,000 in cash." Reporting officials in the Northern District of New York described a federal wiretap in use for 33 days in a narcotics investigation that resulted in 11 arrests, along with the seizure of 11 vehicles, 11 weapons, and $1.3 million in cash. Incriminating communications obtained in a wiretap in the Western District of Texas produced the seizure of more than nine tons of marijuana plus four vehicles. Surveillance of fax communications at a financial institution reported in the District of New Jersey contributed to one arrest and the seizure of $20.8 million from 39 accounts. In the Eastern District of New York, reporting officials noted that intercepts from a racketeering investigation "were essential to obtaining convictions and saving the victim from a beating."

On the state level, the assistant district attorney in Montgomery County, Pennsylvania, reported that the information obtained in a wiretap with microphone surveillance in operation for 56 days "provided the crucial evidence to establish probable cause to search 28 locations, where we found narcotics and proceeds of trafficking; the conversations established the nature, extent and



identity of the conspiracy." The district attorney in Rockland County, New York, noted that interceptions in a wiretap involving cellular telephone and electronic pager surveillance conducted over 120 days in a narcotics investigation "were vital in obtaining the evidence needed to indict and convict the members of a narcotics organization [that] would otherwise not have been able to be dismantled." In Oklahoma, the district attorney in Comanche County reported that a wiretap in use for 41 days in an investigation of methamphetamine trafficking led to the conviction of seven of nine persons arrested. The report stated that the surveillance "yielded information about where and when traffickers were meeting to exchange cash, drugs, and information; provided details of how the drug network operated and where; identified principals; and allowed surveillance of meetings and opportunities to arrest." In San Bernardino County, California, officials reported that surveillance of a standard telephone for 12 days enabled investigators to gain the full scope and involvement of all suspects on a nine year-old murder investigation.

Table 6 presents the numbers of persons arrested and convicted as a result of interceptions reported as terminated in 2002. As of December 31, 2002, a total of 3,060 persons had been arrested based on interceptions of wire, oral, or electronic communications. Wiretaps terminated in 2002 resulted in the conviction of 493 persons as of December 31, 2002, which was 16 percent of the number of persons arrested. Federal wiretaps were responsible for 50 percent of the arrests and 28 percent of the convictions arising from wiretaps during 2002. A state wiretap in Middlesex County, New Jersey, resulted in the most arrests of any intercept terminated in 2002. This wiretap was the lead wiretap of eight intercepts authorized for use in narcotics and gambling investigations that led to the arrest of 136 persons. The Northern District of Ohio produced the most arrests of any federal wiretap when an intercept used in a narcotics investigation yielded the arrests of 50 persons. The leader among state intercepts in producing convictions was a wiretap that took place in Rockland County, New York, which was used in a narcotics investigation that led to the conviction of 31 of the 47 persons arrested. The largest number of convictions reported from a federal wiretap terminated in 2002 occurred in the District of New Jersey, where a wiretap used in a narcotics conspiracy investigation resulted in 15 arrests and 15 convictions.

Because criminal cases involving the use of surveillance may still be under active investigation or prosecution, the final results of many of the wiretaps concluded in 2002 may not have been reported. Prosecutors will report the additional 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 and B-2 of subsequent volumes of the *Wiretap Report*.

Summary of Reports for Years Ending December 31, 1992 Through 2002

Table 7 provides information on intercepts reported each year from 1992 to 2002. This table specifies the number of intercept applications requested, 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 1992 to 2002, the number of intercept applications authorized increased 48 percent. The majority of wiretaps involved drug-related investigations, ranging from 69 percent of all applications authorized in 1992 to 77 percent in 2002.

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 2002, a total of 2,458 arrests, 2,616 convictions, and additional costs of $12,262,988 arose and were reported from wiretaps completed in previous years. Table 8 summarizes additional prosecution activity by jurisdiction from supplemental reports on intercepts terminated in the years noted. Nearly half of the supplemental reports of additional activity in 2002 involved wiretaps terminated in 2001. Of all supplemental arrests, convictions, and costs reported in 2002, intercepts concluded in 2001 led to 54 percent of arrests, 50 percent of convictions, and 75 percent of expenditures. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1992 through 2002.