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, 2000, and December 31, 2000, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 1,190 intercepts authorized by federal and state courts were completed in 2000, a decrease of 5 percent compared to the number terminated in 1999. In 2000, wiretaps installed were in operation on average 15 percent fewer days per wiretap than in 1999, and the number of intercepts per order was 8 percent lower, but the average number of incriminating communications intercepted per wiretap increased 3 percent.

Public Law 106-197 amended 18 U.S.C. 2519(2)(b) to require that beginning with the *2000 Wiretap Report,* 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. In 2000, encryption was reported to have been encountered in 22 wiretaps; 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 2000. 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 2000 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 2000 compared to 1999. The AO is grateful for the cooperation and the prompt responses we received from many officials around the nation.

Leonidas Ralph Mecham
Director

April 2001

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.

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

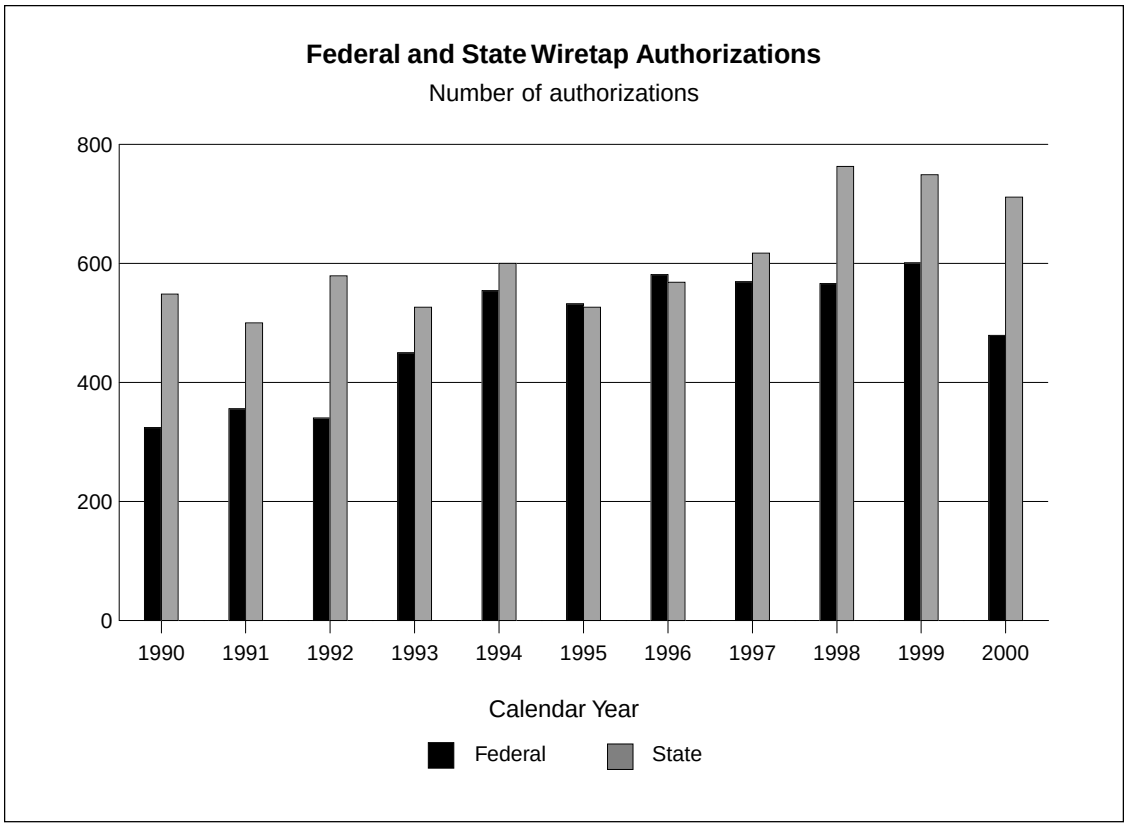
installation of the intercept device. Under 18 U.S.C. 2519(2), prosecuting officials must file supplementary reports on additional court or police activity that occurs as a result of intercepts reported in prior years. Appendix Tables A-2 and B-2 describe the additional activity reported by prosecuting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

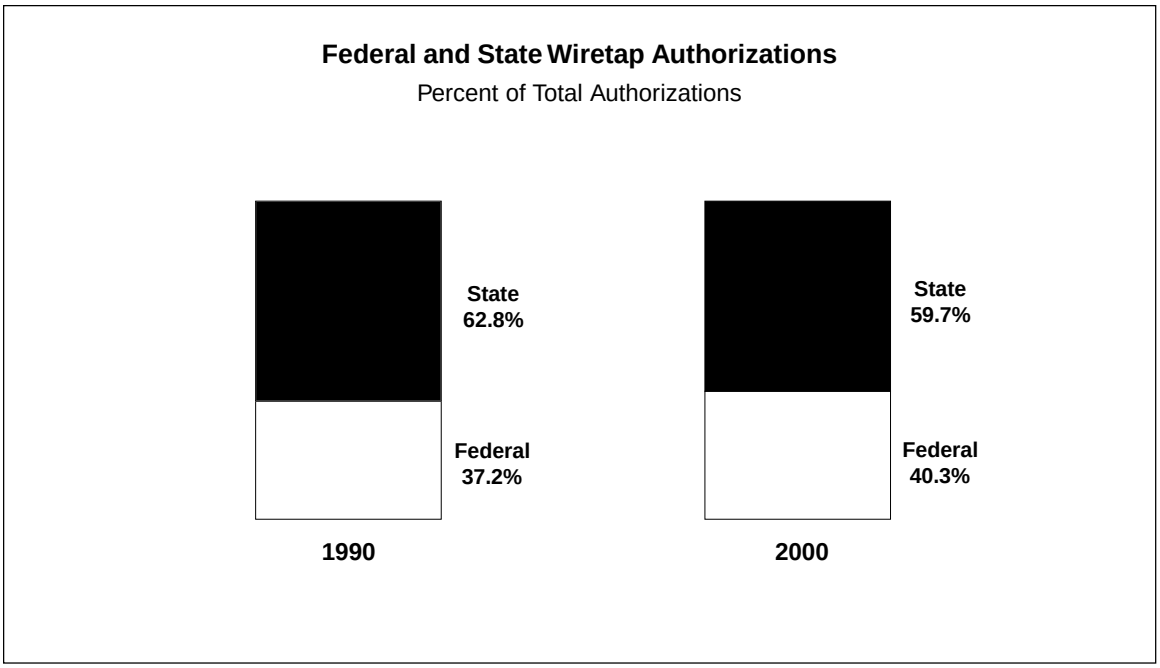
Table 1 shows that 45 jurisdictions (the federal government, the District of Columbia, the Virgin Islands, and 42 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. During 2000, a total of 26 jurisdictions reported using at least one of 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 2000 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*.

Beginning with the *2000 Wiretap Report,* the assignment of reporting numbers to federal wiretaps has been modified so that a comparable numbering system is used for both federal and state wiretaps. Each year, some reports are submitted on wiretaps that were terminated in prior years but, because they had been part of ongoing investigations, were not reported along with other wiretaps terminated the same year. In previous *Wiretap Reports,* the numbering system for federal wiretaps blended wiretaps for the current year with newly reported wiretaps that had been terminated in prior years, which made it difficult to track data from year to year. For this year's report, comparisons with last year's totals are based on wiretaps that were terminated during that year. That is, for 1999, comparisons are based not on





the previously reported total of 1,350 wiretaps, which includes 98 federal wiretaps that actually were terminated in prior years, but on a total that includes only the 1,252 wiretaps that were completed in 1999.

The number of wiretaps reported decreased 5 percent in 2000. A total of 1,190 applications were authorized in 2000, including 479 submitted to federal judges and 711 to state judges. Judges approved all applications. The number of applications approved by both federal and state judges in 2000 each decreased 5 percent compared to the number approved during 1999.[1] Wiretap applications in New York (349 applications), California (88 applications), New Jersey (45 applications), Pennsylvania (43 applications), Florida (43 applications), and Illinois (41 applications) accounted for 86 percent of all authorizations approved by state judges.

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 length 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 2000, the average length of an original authorization was 28 days, up from 27 days in 1999. A total of 926 extensions were requested and authorized in 2000 (a decrease of 32 percent). The average length of an extension was 28 days, down from 29 days in 1999. The longest federal intercept occurred in the Central District of California, where the original 30-day order was extended 10 times to complete a 308-day wiretap used in a narcotics investigation. Among state wiretaps terminating during 2000, the longest was used in a narcotics investigation in Queens County, New York; this wiretap required a 30-day order to be extended nine times to keep the intercept in operation 300 days. In contrast, 19 federal intercepts and 48 state intercepts each were in operation for less than a week.

Locations

Wire, oral, and electronic communications technologies have changed dramatically over the past 10 years. To reflect these changes, the location categories used in this year's *Wiretap Report*

have been revised. As a result, location data in this year's report are not comparable to data for earlier years.

The most common location specified in wiretap applications authorized in 2000 was "portable device, carried by/on individual," a category included for the first time this year in Table 2. 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 previously provided. Table 2 shows that in 2000, a total of 60 percent (715 wiretaps) of all intercepts authorized were for portable devices such as these, which are not limited to fixed locations.

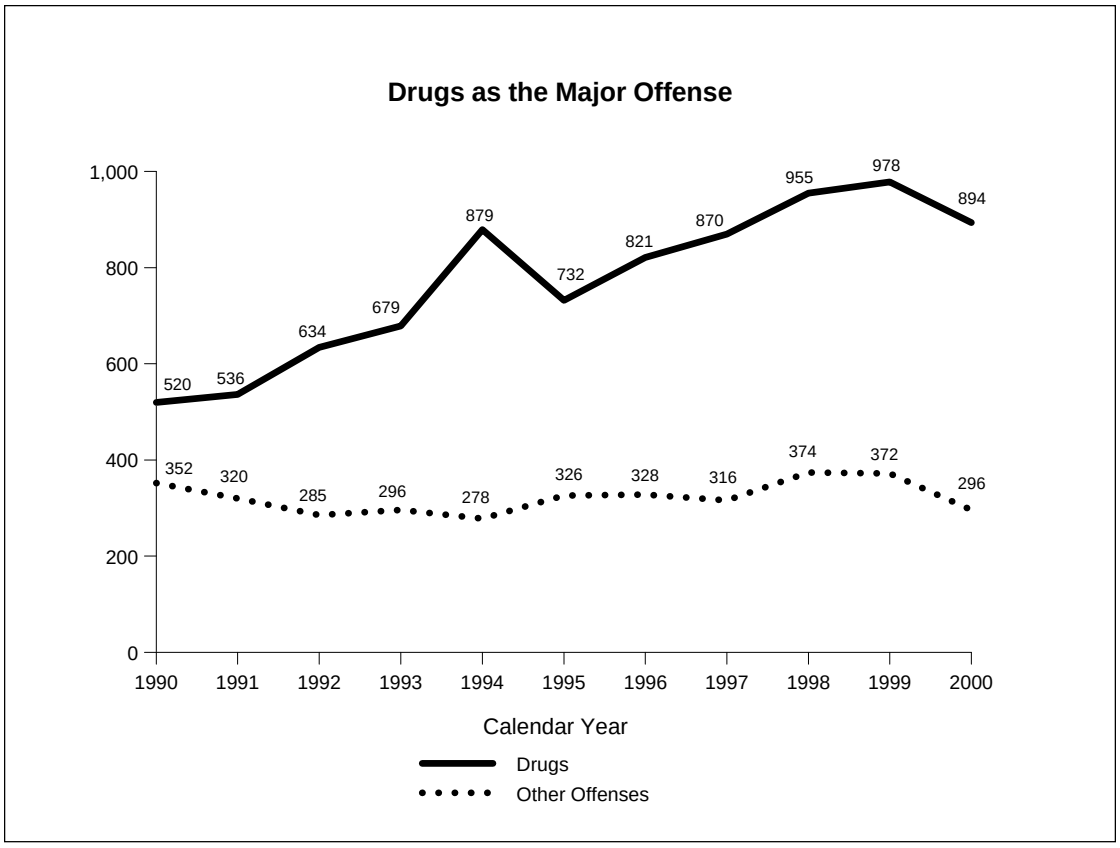
The next most common location cited for the placement of wiretaps in 2000 was a "personal residence," a type of location that includes single-family houses, as well as row houses, apartments, and other multi-family dwellings. Table 2 shows that in 2000 a total of 21 percent (251 wiretaps) of all intercept devices were authorized for personal residences. Four percent (53 wiretaps) were authorized for business establishments such as offices, restaurants, and hotels. Combinations of locations were cited in 109 federal and state applications (9 percent of the total) in 2000. Finally, 3 percent (35 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 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 2000, authorizations for 27 wiretaps indicated approval with a relaxed specification order under 18 U.S.C. 2518(11). Federal authorities reported that roving wiretaps were approved for seven investigations; three were authorized for use in drug offense investigations, one in a murder investigation, one in a gambling investigation, one in a racketeering investigation, and one in a firearms investigation. On the state level, 20 roving wiretaps were reported; 60 percent (12 applications) were authorized for use in drug offense investigations, 10 percent (2 applications) in bribery investigations, and the remainder (six applications) in investigations of other offenses.

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 75 percent of all applications for intercepts (894 wiretaps) authorized in 2000 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 Texas (27 applications) and the Northern District of Illinois (26 applications). On the state level, the New York City Special Narcotics Bureau obtained authorizations for 108 drug-related intercepts, which accounted for the highest percentage (21 percent) of all drug-related intercepts reported by state or local jurisdictions in 2000. Nationwide, racketeering (76 orders), homicide/assault (72 orders), and gambling (49 orders) were specified in 6 percent, 6 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 2000. Judges submitted 23 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 1,190 communication interceptions authorized in 2000, intercept devices were installed in conjunction with a total of 1,139 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 2000, installed wiretaps were in operation an average of 42 days, a 15 percent decrease from the average number of days wiretaps were in operation in 1999. The average number of interceptions per day reported by all jurisdictions in 2000 ranged from less than 1 to over 700. The most active federal intercept occurred in the Northern District of Ohio, where a 60-day fraud investigation installation involved 180 agent workdays and resulted in an average of 346 interceptions per day. For state authorizations, the most active investigation was a 35-day bribery investigation in New York County, New York, that produced an average of 713 intercepts per day. Nationwide, in 2000 the average number of persons whose communications were intercepted per order in which intercepts were installed was 196, essentially the same as the average number in 1999 (which was 195 persons). The average number of communica-

tions intercepted was 1,769 per wiretap; an average of 402 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order increased from 20 percent of interceptions in 1999 to 23 percent in 2000.

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.

In recent years, many wiretaps involving the interception of communications via cellular telephones were reported under the category of "electronic" wiretaps. However, cellular telephones that carry voice conversations are considered "wire communications" under 18 U.S.C. 2510 (1), which states that "'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station)." Beginning with the *2000 Wiretap Report,* all wiretaps involving the interception of cellular telephones are categorized as "wire" interceptions.

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 81 percent (927 cases) of intercepts installed in 2000. Of those, 691 wiretaps involved cellular/mobile telephones, either as the only type of device under surveillance (578 cases) or in combination with one or more other types (113 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 8 percent (89 cases) of intercepts installed in 2000. Microphones were used in 5 percent of intercepts (52 cases). A combination of surveillance methods was used in 6 percent of intercepts (71 cases).

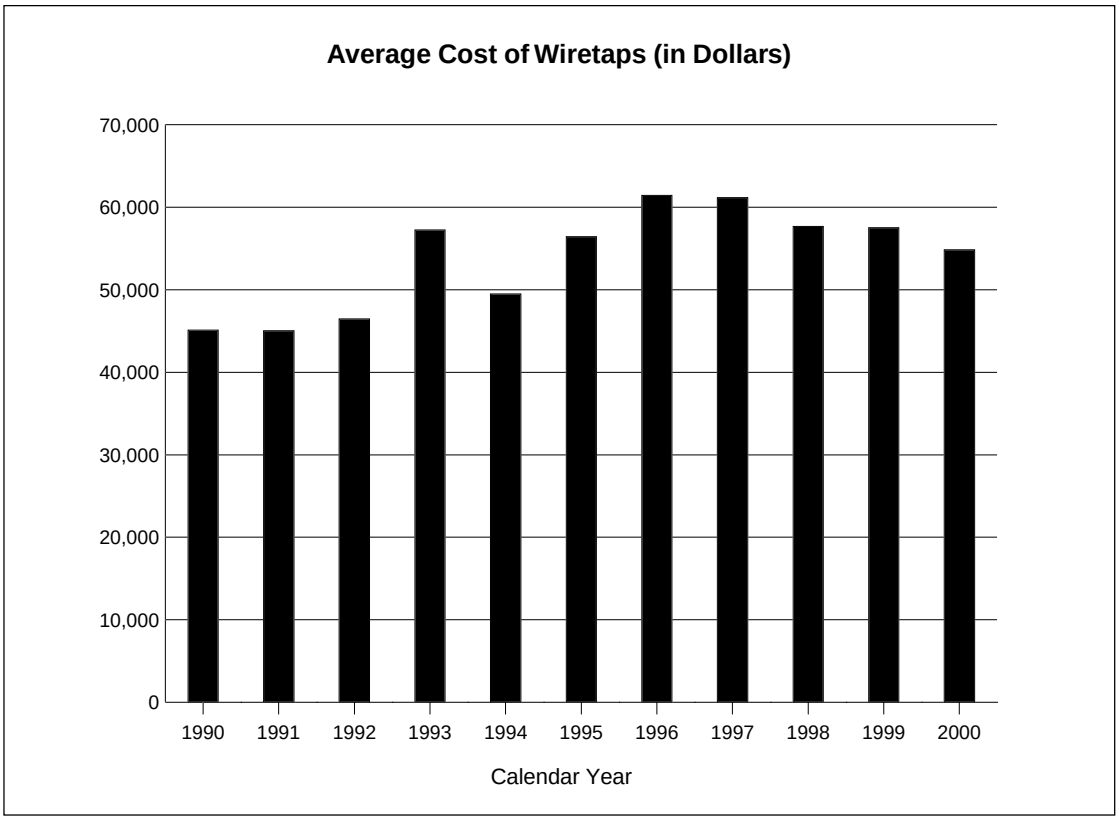
Public Law 106-197 amended 18 U.S.C. 2519(2)(b) to require that beginning with the *2000 Wiretap Report,* reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2000, no federal wiretaps reported that encryption was encountered. For state and local jurisdictions, encryption was reported to have been encountered in 22 wiretaps in 2000; however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted.

Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 2000. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,080 authorizations for which reports included cost data. The average cost of intercept devices installed in 2000 was $54,829, down 5 percent from the average cost in 1999. For federal wiretaps for which expenses were reported in 2000, the average cost was $63,767, a 13 percent decrease from the average cost in 1999. However, the average cost of a state wiretap increased 11 percent to $47,993 in 2000. 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 Central District of California reported a federal wiretap that involved cellular telephone and digital pager surveillance



in a narcotics conspiracy investigation that led 15 persons to plead guilty; in addition, the reporting officials noted that this wiretap "resulted in the seizure of 40 tons of marijuana, 8 kilos of cocaine, 16 pounds of methamphetamine, 22 firearms, 5 vehicles, and $72,209." Reporting officials in the Northern District of Illinois described a federal wiretap in use for 19 days in a narcotics investigation that resulted in 12 arrests and the seizure of 50 kilos of cocaine, $1.5 million in cash, and 10 vehicles. On the state level, the prosecuting attorney in Latah County, Idaho, reported that, as part of a murder investigation, the information obtained in a wiretap of a standard telephone in a jail "was instrumental in the State obtaining convictions for two counts of first degree murder, first degree arson, conspiracy to commit murder and arson, and preparing false evidence. Among other things, the intercepted communications revealed attempts by the defendant to create fictitious alibis, giving us the opportunity to thoroughly investigate and rebut the same at trial." The San Bernardino District Attorney's office in California reported that a 58-day wiretap approved as part of a narcotics investigation resulted in the arrest of 11 persons, 5 of whom were convicted, adding that "without the wiretap, the head of this distribution organization and his chief co-conspirators would not have been convicted. Conventional investigative techniques would have only resulted in the conviction of the organization's 'mules.'" The State Attorney's office in New Haven County, Connecticut, reported that a wiretap in use for 15 days in a narcotics investigation resulted in six arrests and one subsequent conviction, stating that the interceptions "were successful in identifying upper-level suppliers and buyers of narcotics, leading to the seizure of narcotics, weapons, and assets with accompanying arrests that most likely would have been unobtainable through the use of normal investigative procedures." The office of the Attorney General in Oklahoma indicated that a 34-day wiretap investigating the manufacture of methamphetamine resulted in 27 arrests and the subsequent conviction of 14 individuals; the Attorney General noted that "none of these convictions could have been achieved without evidence obtained from wire interception."

Table 6 presents the numbers of persons arrested and convicted as a result of interceptions reported as terminated in 2000. As of December 31, 2000, a total of 3,411 persons had been

arrested based on interceptions of wire, oral, or electronic communications, 22 percent (736 persons) of whom were convicted (an increase from the 1999 conviction rate of 15 percent, returning to a percentage rate closer to the 1998 conviction rate of 26 percent). Federal wiretaps were responsible for 52 percent of the arrests and 48 percent of the convictions during 2000. A wiretap in the District of Hawaii resulted in the most arrests of any intercept in 2000. This wiretap, which was the lead wiretap of three used in a narcotics investigation, led to the arrest of 50 persons. A wiretap in the Eastern District of Louisiana produced the most convictions of any wiretap when an intercept used in a drug investigation resulted in the conviction of 33 of the 34 persons arrested. The leader among state intercepts in producing arrests and convictions was a wiretap that took place in Maricopa County, Arizona, and was the lead wiretap of two used in a drug investigation. This wiretap resulted in 47 arrests and 21 convictions. Because criminal cases involving the use of surveillance may still be under active investigation, the results of many of the intercepts concluded in 2000 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 and B-2 of subsequent volumes of the *Wiretap Report*.

Summary of Reports for Years Ending December 31, 1990 Through 2000

Table 7 provides information on intercepts reported each year from 1990 to 2000. 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 1990 to 2000, the number of intercept applications authorized increased 36 percent. The majority of wiretaps involved drug-related investigations, ranging from 60 percent of all applications authorized in 1990 to 75 percent in 2000.

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 2000, a total of 2,264 arrests, 2,181 convictions, and additional costs of $8,734,348 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 2000 involved wiretaps terminated in 1999. Intercepts concluded in 1999 led to 71 percent of arrests, 61 percent of convictions, and 82 percent of expenditures reported in 2000 for wiretaps terminated in prior years. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1990 through 2000.

Endnote

[1] In the *1999 Wiretap Report,* 601 federal wiretaps and 749 state wiretaps were reported for 1999. However, of the 601 federal wiretaps, 503 had been terminated in 1999, whereas 98 had been concluded in prior years but not reported until 1999 because they had been part of ongoing investigations. For consistency with the new method of counting wiretaps in the *2000 Wiretap Report,* percentage changes between 1999 and 2000 have been calculated based solely on wiretaps that ended in each of those years.