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, 2004, and December 31, 2004, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 1,710 intercepts authorized by federal and state courts were completed in 2004, an increase of 19 percent compared to the number terminated in 2003. The number of applications for orders by federal authorities rose 26 percent to 730. The number of applications reported by state prosecuting officials grew 13 percent to 980, with 19 state jurisdictions providing reports, four fewer than in 2003, but equal to the number for 2002. Wiretaps installed were in operation an average of 43 days per wiretap in 2004 compared to 44 days in 2003. The average number of persons whose communications were intercepted increased from 116 per wiretap order in 2003 to 126 per order in 2004. The average percentage of intercepted communications that were incriminating was 21 percent in 2004, compared to 33 percent in 2003.

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. In 2004, two instances were reported of encryption's being encountered on wiretaps. One federal jurisdiction and one state jurisdiction each reported that encryption was encountered in a wiretap terminated in 2004; however, in both cases, the encryption was reported to have not 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 2004. 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 2004 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 percentage of missing state and local prosecutors' reports was 3 percent, the same as in 2003. 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 2005

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

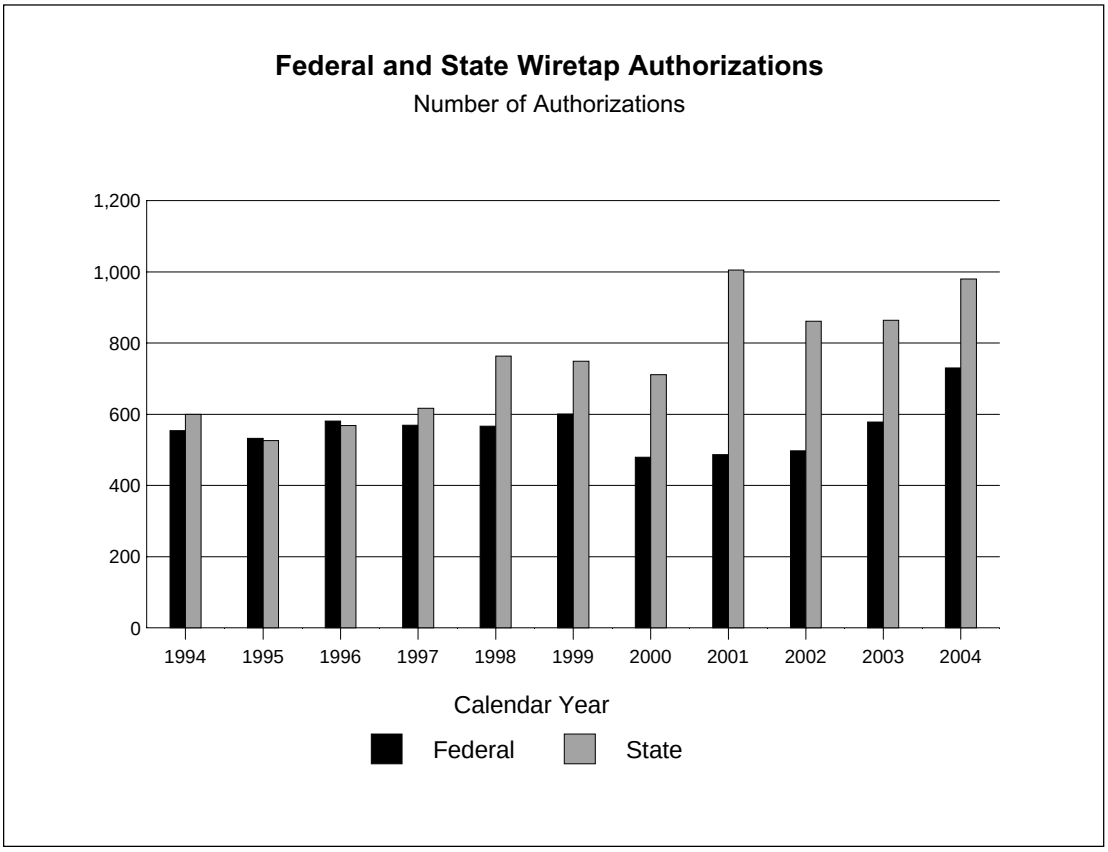
additional court or police activity that occurs as a result of intercepts reported in prior years. Appendix Tables A-2 and B-2 describe the additional activity reported by prosecuting officials in their supplementary reports.

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 2004, 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 2004 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.*

The number of wiretaps reported increased 19 percent in 2004. A total of 1,710 applications were authorized in 2004, including 730 submitted to federal judges and 980 to state judges. Judges approved all applications. Compared to the number approved during 2003, the number of applications approved by federal judges in 2004 increased 26 percent, and the number of applications approved by state judges rose 13 percent. Wiretap applications in New York (347 applications), California (180 applications), New Jersey (144 applications), and Florida (72 applications) accounted for 76 percent of all applications approved by state judges. The number of states reporting wiretap activity was lower than the number for last year (19 states reported such activity in 2004, compared to 23 in 2003) but equal to the number for 2002. Eighty-five separate state jurisdictions submitted reports for 2004, which is 17 fewer than the total for 2003, but 5 more than the total for 2002.



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 2004, the average length of an original authorization was 28 days, one day fewer than in 2003. A total of 1,341 extensions were requested and authorized in 2004, an increase of 17 percent. The average length of an extension was 28 days, one fewer than in 2003. The longest federal intercept occurred in the Northern District of Illinois, where an original 30-day order was extended 12 times to complete a 390-day wiretap used in a racketeering investigation. Among state wiretaps terminating during 2004, the longest was used in a narcotics investigation conducted in Queens County, New York; this wiretap, also in use for 390 days, required a 30-day order to be extended 12 times. In contrast, 24 federal intercepts and 59 state intercepts each were in operation for less than a week.

Locations

The most common location specified in wiretap applications authorized in 2004 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 fit readily into the location categories provided prior to 2000. Since that time, the proportion of wiretaps involving fixed locations has declined as the use of mobile communications devices has become more prevalent. Table 2 shows that in 2004, a total of 88 percent (1,507 wiretaps) of all intercepts authorized involved portable devices such as these, which are not limited to fixed locations. This is an increase of 7 points over the percentage in 2003, when 81 percent of all intercepts involved portable devices.

The next most common specific location for the placement of wiretaps in 2004 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 2004, a total of 5 percent (83 wiretaps) of all intercept devices were authorized for personal residences. Two percent (30 wiretaps) were authorized for business establishments such as offices, restaurants, and hotels. Combinations of locations were cited in 65 federal and state applications (4 percent of the total) in 2004. One percent (22 wiretaps) were authorized for "other" locations, which included such places as prisons, pay telephones in public areas, and motor vehicles.

Pursuant to 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) to provide 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 2004, an authorization for one wiretap indicated approval with a relaxed specification order, meaning it was considered a roving wiretap. This is a decrease from 2003, when six wiretaps were reported as roving wiretaps. The roving wiretap approved in 2004 was a federal wiretap used in a narcotics investigation; no roving wiretaps were reported by state authorities.

Offenses

Violations of drug laws and racketeering laws were the two most prevalent types of offenses investigated through communications intercepts. Gambling was the third most frequently recorded offense category, and homicide/assault the fourth. Table 3 indicates that 76 percent of all applications for intercepts (1,308 wiretaps) authorized in 2004 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 (95 applications), the Northern District of Illinois (51 applications), and the Central District of California (42 applications). On the state level, the largest number of drug-related intercepts was reported in Queens County, New York (83 applications), followed by Los Angeles County, California (75 applications) and the New York City Special Narcotics Bureau (73 applications). Nationwide, racketeering (138 orders) and gambling (90 orders) were specified in 8 percent and 5 percent of applications, respectively, as the most serious offense under investigation. The categories of homicide/assault (48 orders) and larceny/theft/robbery (39 orders) were specified in 3 percent and 2 percent of applications, respectively.

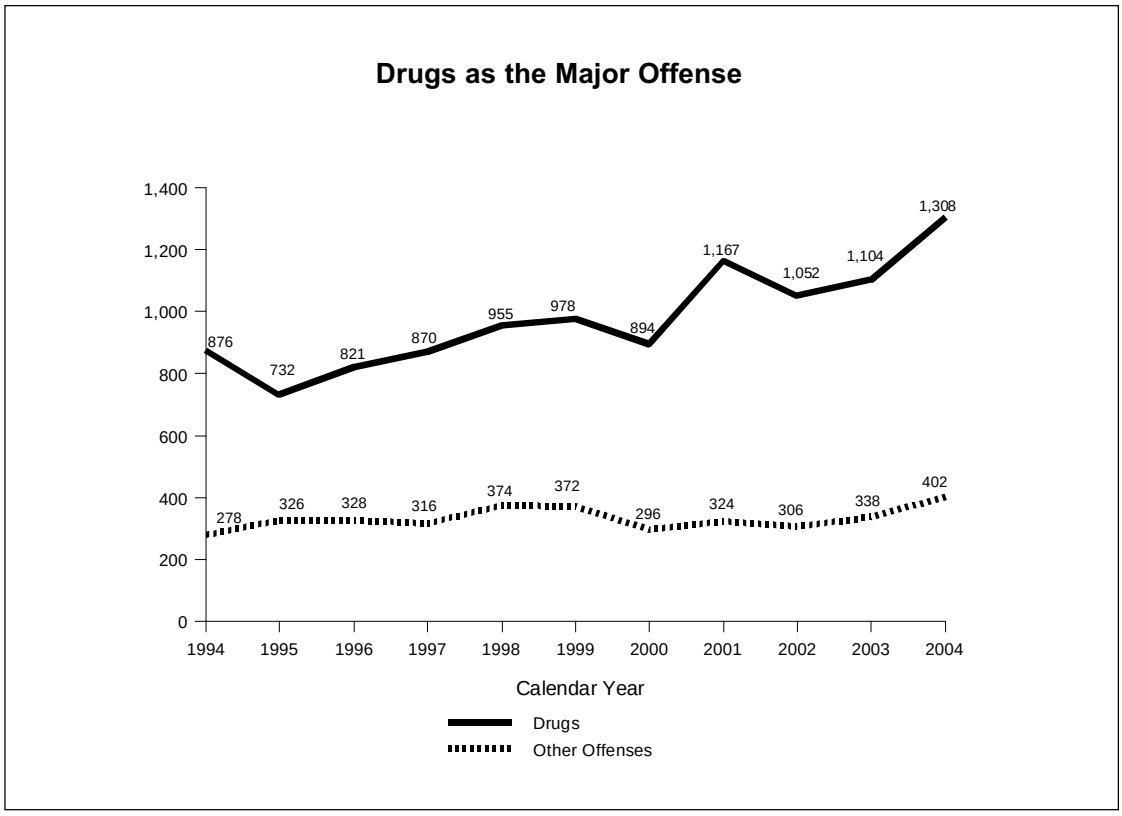
Summary and Analysis of Reports by Prosecuting Officials

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 2004. Judges submitted 52 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 1,710 communication interceptions authorized in 2004, reports submitted by prosecutors indicated that intercept devices were installed and results were reported in conjunction with a total of 1,633 orders. As shown in Table 2, orders for 25 wiretaps were approved for which no wiretaps actually were installed, and results from 52 wiretap orders were not available for reporting by the prosecutors. 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 2004, installed wiretaps were in operation an average of 43 days, one day less than the average number of days wiretaps were in operation in 2003. The most active federal wiretap occurred in the District of New Jersey, where a counterfeiting investigation involving the interception of computer messages resulted in the interception of 206,444 messages over 30 days. The second most active federal intercept, also a computer wiretap, occurred in the Southern District of New York as part of a 30-day racketeering investigation and resulted in a total of 107,779 interceptions. The next most active federal wiretaps involved cellular telephone intercepts: a 30-day narcotics investigation in the Northern District of Illinois with an average of 476 interceptions per day, and a 60-day narcotics investigation in the District of Colorado with an average of 437 interceptions per day. For state authorizations, two jurisdictions reported wiretaps that produced an average of more than 600 intercepts per day: a wiretap used in a 30-day narcotics investigation in Oklahoma County, Oklahoma, with an average of 681 intercepts per day, and a 30-day narcotics investigation in Suffolk County, New York, with an average of 619 intercepts per day. Nationwide, in 2004 the average number of persons whose communications were intercepted per order in which intercepts were installed was 126, and the average number of communications intercepted was 3,017



per wiretap. An average of 619 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order was 21 percent in 2004, compared to 33 percent in 2003.

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.

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 (land line, cellular, cordless, and mobile). Telephone wiretaps accounted for 94 percent (1,530 cases) of intercepts installed in 2004. Of those, 1,480 wiretaps involved cellular/mobile telephones, either as the only type of device under surveillance (1,406 cases) or in combination with other types of telephones (74 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 2 percent (38 cases) of intercepts installed in 2004; 20 of these involved electronic pagers, 12 involved computers, and 6 involved other electronic devices such as fax machines. Oral wiretaps including microphones were used in 2 percent of intercepts (37 cases). A combination of surveillance methods was used in 2 percent of intercepts (28 cases); of these combination intercepts, 93 percent (26 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

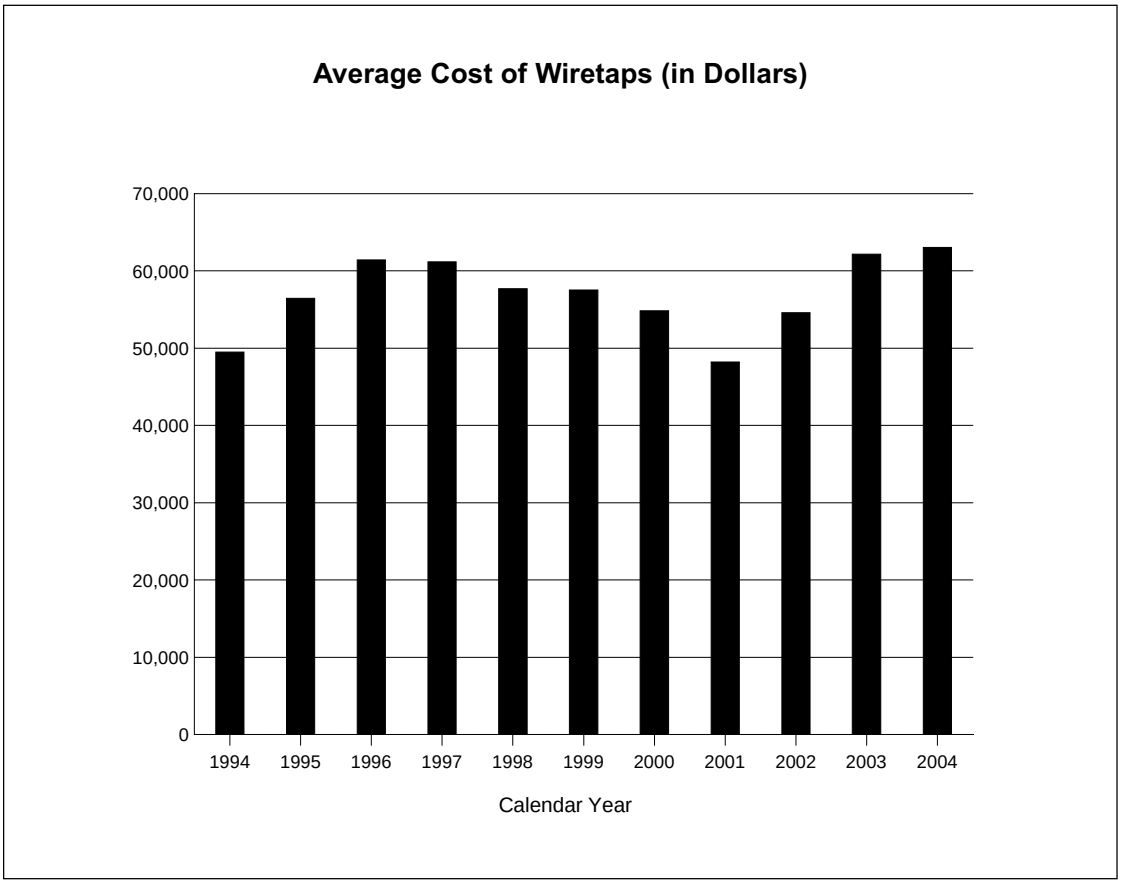
encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2004, one instance was reported of encryption encountered during a federal wiretap; however, the encryption did not prevent law enforcement officials from obtaining the plain text of the communications intercepted. One state jurisdiction reported that encryption was encountered in a wiretap terminated in 2004, but the encryption did not prevent 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 2004. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,559 authorizations for which reports included cost data. The average cost of intercept devices installed in 2004 was $63,011, up 1 percent from the average cost in 2003. For federal wiretaps for which expenses were reported in 2004, the average cost was $75,527, a 5 percent increase from the average cost in 2003. The average cost of a state wiretap fell 3 percent to $52,490 in 2004. For additional information, see Appendix Tables A-1 (federal) & B-1 (state).

Arrests and Convictions

Table 6 presents the numbers of persons arrested and convicted as a result of interceptions reported as terminated in 2004. As of December 31, 2004, a total of 4,506 persons had been arrested based on interceptions of wire, oral, or electronic communications, 23 percent more than in 2003. Wiretaps terminated in 2004 resulted in the conviction of 634 persons as of December 31, 2004, which was 14 percent of the number of persons arrested. Federal wiretaps were responsible for 53 percent of the arrests and 29 percent of the convictions arising from wiretaps during 2004. A federal wiretap in the Western District of Texas that resulted in the most arrests of any intercept terminated in 2004 was the lead wiretap of three intercepts authorized for a bribery investigation



that led to the arrest of 270 persons. Middlesex County, New Jersey, reported the most arrests of any state wiretap; the lead wiretap of two intercepts used in a narcotics investigation there yielded the arrest of 97 persons. The leader among federal intercepts in producing convictions was a wiretap that was the lead wiretap of three intercepts authorized in the District of Connecticut for a narcotics investigation, which led to the conviction of 32 of the 44 persons arrested. Two state jurisdictions each reported an interception producing 26 convictions, tying for the largest number of convictions arising from a state wiretap terminated in 2004. A wiretap used in a narcotics investigation in San Diego County, California, resulted in the conviction of 26 of the 34 persons arrested, and a wiretap that was the lead wiretap of three used in a narcotics investigation in the Fourth Judicial Circuit (Duval), Florida, led to the conviction of 26 of the 33 persons arrested.

Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. The District of Maryland reported that a federal wiretap involving cellular telephone surveillance during a narcotics conspiracy investigation led to 15 arrests and 7 convictions; in addition, the reporting officials stated that this wiretap "resulted in the seizure of 50 kilos of cocaine, 11 kilos of heroin, 3 vehicles, 15 weapons, and $2,600,000 in cash." Reporting officials in the Central District of California described a federal wiretap in use for 60 days in a narcotics importation investigation that resulted in 4 arrests, along with the seizure of 2 tons of marijuana, 10 vehicles, 4 weapons, and $2,161,530 in cash. Incriminating communications obtained from a wiretap in the Middle District of North Carolina produced 11 arrests and the seizure of 9 vehicles, 20 weapons, 23 kilos of cocaine, and $1,764,209 in cash. Surveillance of cellular telephone communications reported by the Southern District of California contributed to 45 arrests and the seizure of 16 pounds of "ice" methamphetamine, 6 kilos of cocaine, 40 pounds of marijuana, 2 indoor marijuana-growing operations, 26 weapons, 7 vehicles, and $1,167,000 in cash.

On the state level, officials in Los Angeles County, California, reported that a cellular telephone wiretap in use for 11 days led to the arrest of conspirators planning to murder a police officer and that "weapons and masks intended for this crime were seized based on information captured on the wire." The district attorney in Franklin County, New York, reported that interceptions obtained from a cellular telephone wiretap conducted over 30 days in a money laundering investigation "were critical to surveillance of a large drug conspiracy in a rural area not conducive to physical surveillance" and resulted in nine arrests. In Georgia, the Gwinnett County district attorney's office reported that a wiretap in use for one day during a kidnapping investigation permitted the interception of communications made by the kidnappers as they used the victim's cellular telephone until the victim was released. In San Bernardino County, California, officials reported that the surveillance of a cellular telephone for 340 days in a narcotics investigation "provided the evidence which has made it possible to prosecute and convict international narcotics traffickers."

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 2004 may not have been reported. Prosecutors will report 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, 1994 Through 2004

Table 7 provides information on intercepts reported each year from 1994 to 2004. 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 1994 to 2004, the number of intercept applications authorized increased 48 percent. The majority of wiretaps consistently have been used for drug crime investigations, which accounted for 76 percent of

intercept applications in 2004. During the past 10 years, the percentage of drug-related wiretaps has ranged from 69 percent to 78 percent of all authorized applications.

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 2004, a total of 2,153 arrests, 1,683 convictions, and additional costs of $19,112,753 arose from and were reported for wiretaps completed in previous years. Table 8 summarizes additional prosecution activity by jurisdiction from supplemental reports on intercepts terminated in the years noted. Sixty-two percent of the supplemental reports of additional activity in 2004 involved wiretaps terminated in 2003. Of all supplemental arrests, convictions, and costs reported in 2004, intercepts concluded in 2003 led to 77 percent of arrests, 59 percent of convictions, and 94 percent of expenditures. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1994 through 2004.