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, 2007, and December 31, 2007, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 2,208 intercepts authorized by federal and state courts were completed in 2007, an increase of 20 percent compared to the number terminated in 2006. The number of applications for orders by federal authorities fell less than 1 percent to 457. The number of applications reported by state prosecuting officials grew 27 percent to 1,751, with 24 states providing reports, 1 more than in 2006. Installed wiretaps were in operation an average of 44 days per wiretap in 2007, compared to 40 days in 2006. The average number of persons whose communications were intercepted decreased from 122 per wiretap order in 2006 to 94 per wiretap order in 2007. The average percentage of intercepted communications that were incriminating was 30 percent in 2007, compared to 20 percent in 2006.

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 2007, no instances were reported of encryption encountered during any federal or state wiretap.

The appendix tables of this report list all intercepts reported by judges and prosecuting officials for 2007. 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 2007 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. A total of 56 state and local prosecutors' reports were missing in 2007, compared to 96 in 2006. 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.

James C. Duff
Director

April 2008

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 Is-

lands, and 44 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. During 2007, a total of 25 jurisdictions reported using at least one of these three types of surveillance as an investigative tool.

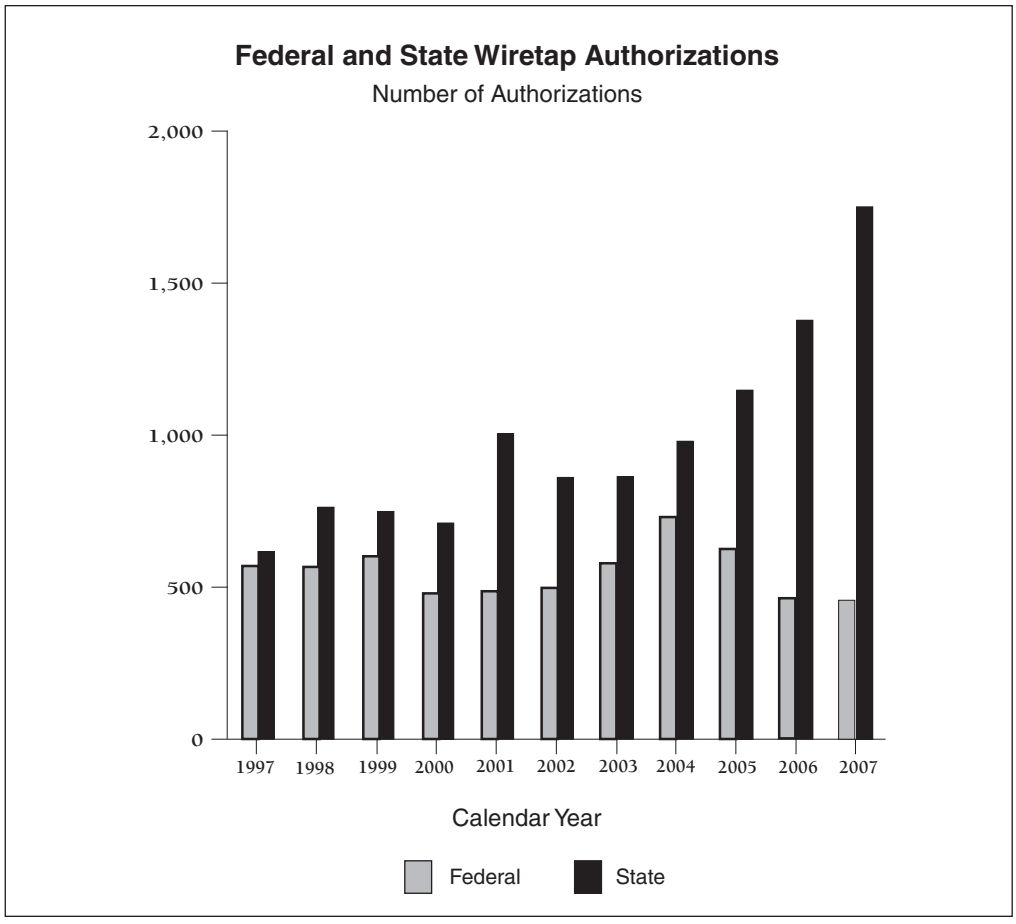
Summary and Analysis of Reports by Judges

Data on applications for wiretaps terminated during calendar year 2007 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 20 percent in 2007. A total of 2,208 applications were reported as authorized in 2007, including 457 submitted to federal judges and 1,751 to state judges. No applications were denied. Compared to the number approved during 2006, the number of applications reported as approved by federal judges in 2007 fell less than 1 percent. The number of applications approved by state judges rose 27 percent. Wiretap applications in California (560 applications), New York (518 applications), New Jersey (200 applications), and Maryland (108 applications) accounted for 79 percent of all applications approved by state judges. The number of states reporting wiretap activity was higher than the number for last year (24 states reported such activity in 2007, compared to 23 in 2006). In 2007, a total of 117 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, which is 13 more than the total for 2006.

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 2007, the average length of an original authorization was 29 days, the same average length as in 2006. A total of 1,701 extensions were requested and authorized in 2007, an increase of 39 percent. The average length of an extension remained unchanged at 29 days. The longest federal intercept occurred in the District of Colorado, where an original 30-day order was extended 7 times to complete a 233-day wiretap used in a narcotics investigation. Among state wiretaps terminating during 2007, the longest was used in a narcotics investigation conducted in Queens County, New York; this wiretap, in use for 556 days, required the original order to be extended 18 times. In contrast, 17 federal intercepts and 60 state intercepts were in operation for less than a week.

Locations

The most common location specified in wiretap applications authorized in 2007 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 2007, a total of 94 percent (2,080 wiretaps) of all intercepts authorized involved portable devices such as these, which are not limited to fixed locations. This is a slight increase from 2006, when 92 percent of all intercepts involved portable devices.

The next most common specific location for the placement of wiretaps in 2007 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 2007, a total of 1 percent (27 wiretaps) of all intercept devices were authorized for personal residences. Combinations of locations were cited in 36 federal and state applications (2 percent of the total). Twenty-eight wiretaps were authorized for "other" locations, which included such places as prisons, pay telephones in public areas, and motor vehicles. Seven wiretaps were authorized for business establishments such as offices, restaurants, and hotels. Together, "other" and business establishments accounted for 2 percent of all intercepts authorized.

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"

Federal Wiretaps

The Department of Justice has indicated that it examined the reported use of wiretaps in federal investigations for this year's report to Congress and has provided the following comments:

> In recent years, to avoid reporting wiretap data involving sensitive and/or sealed matters, the federal law enforcement agencies and the Department of Justice have exercised special scrutiny when submitting information to the Administrative Office of the United States Courts. Statistics indicate that if all intercepts undertaken for federal investigations in 2007 were reported, the *2007 Wiretap Report* would not reflect any decrease in the use of court-approved electronic surveillance by the agencies. Any matters that could not be included in the 2007 data should be reported in future editions of the *Wiretap Report* as soon as the underlying investigations are completed and/or the matters become unsealed.

(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 2007, authorizations for 21 wiretaps indicated approval with a relaxed specification order, meaning they were considered roving wiretaps. This is an increase from 2006, when 15 wiretaps were reported as roving wiretaps. All 21 roving wiretaps were reported by state authorities: 14 were used in narcotics investigations, 6 in racketeering investigations, and 1 in a murder investigation.

Offenses

Violations of drug laws and homicide/assault were the two most prevalent types of offenses investigated through communications intercepts. Racketeering was the third most frequently recorded offense category, and gambling the fourth. Table 3 indicates that 81 percent of all applications for intercepts (1,792 wiretaps) authorized in 2007 cited a drug offense 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 (40 applications), the Eastern District of New York (35 applications), and the Southern District of New York (33 applications). On the state level, the largest numbers of drug-related intercepts were reported by Los Angeles County of California (257 applications), Queens County of New York (162 applications), and San Diego County of California (120 applications). Nationwide, homicide/assault (132 orders) was specified in 6 percent of applications as the most serious offense under investigation. Racketeering (98 orders) was specified in 4 percent of applications as the most serious offense under investigation. The categories of gambling (55 orders) and larceny/theft/robbery (36 orders) each were specified in 2 percent of applications. Two other offense categories in Table 3 with significant totals were corruption (32 orders) and conspiracy (26 orders).

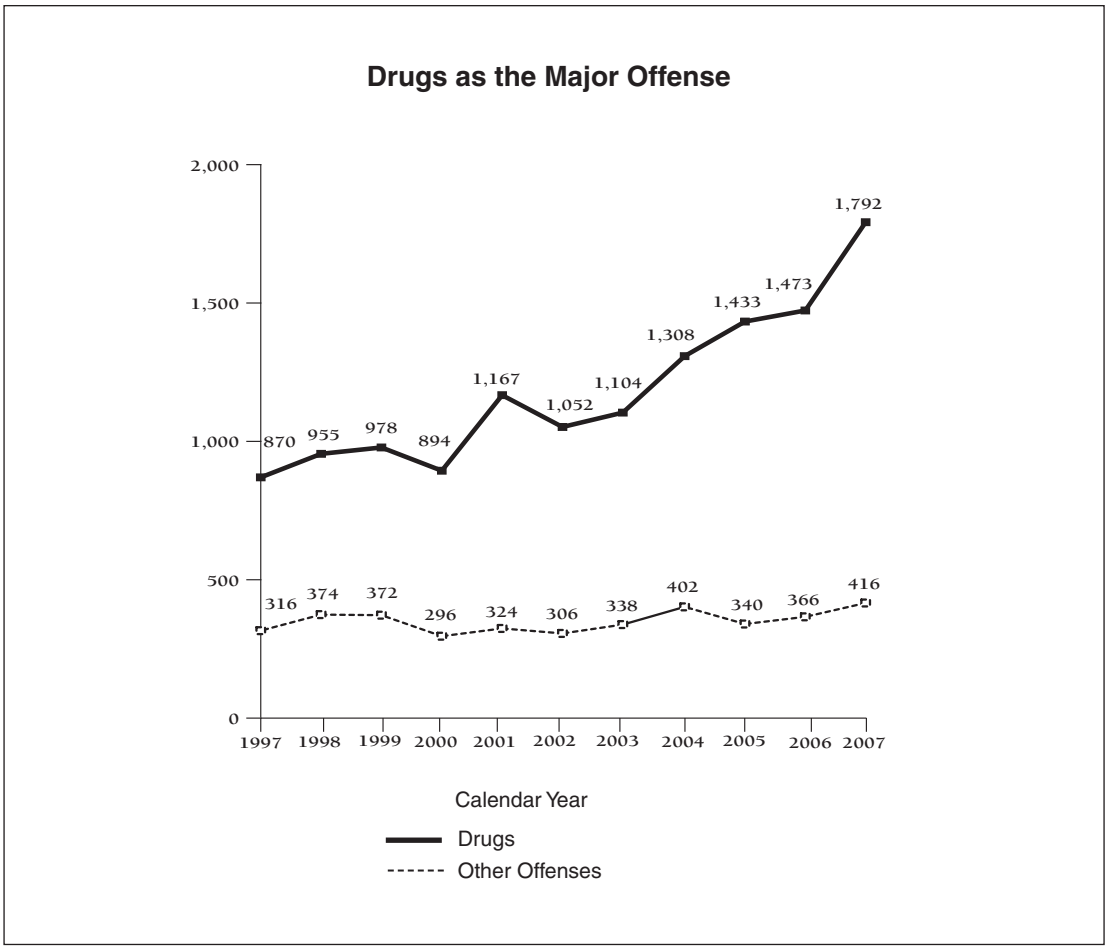
Summary and Analysis of Reports by Prosecuting Officials

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 2007. Judges submitted 56 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 2,208 communication interceptions authorized in 2007, reports submitted by prosecutors indicated that intercept devices were installed and results were reported in conjunction with a total of 2,119 orders. As shown in Table 2, orders for 33 wiretaps were approved for which no wiretaps actually were installed, and results from 56 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 2007, installed wiretaps were in operation an average of 44 days, 4 days longer than the average number of days wiretaps were in operation in 2006. The federal wiretap with the most intercepts occurred in the Western District of Louisiana, where a narcot-



ics investigation involving the interception of cellular telephone communications resulted in the interception of 27,450 messages over 30 days. The federal wiretap with the second highest number of intercepts, also a cellular telephone wiretap, occurred in the Northern District of Illinois as part of a fraud investigation; this wiretap was active for 82 days and resulted in a total of 25,223 interceptions. The federal wiretap with the second highest number of interceptions per day, after the Western District of Louisiana at 915 per day, also involved cellular telephone intercepts. This wiretap lasted 30 days and was used in a narcotics investigation in the District of Utah, which produced an average of 543 interceptions per day.

The state wiretap with the most intercepts occurred in Queens County, New York, where a 363-day wiretap used in a narcotics investigation involving the interception of cellular telephone communications resulted in the interception of 185,600 messages, 100,000 of which were incriminating. Ventura County in California reported the state wiretap with the highest number of interceptions per day. In that case, a 13-day cellular telephone wiretap produced an average of 1,909 intercepts per day for a narcotics investigation. A second wiretap in Ventura County lasted 25 days and generated 992 cellular telephone intercepts per day.

Nationwide, in 2007 the average number of persons whose communications were intercepted per order in which intercepts were installed was 94, and the average number of communications intercepted was 3,106 per wiretap. An average of 920 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order increased from 20 percent in 2006 to 30 percent in 2007.

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.

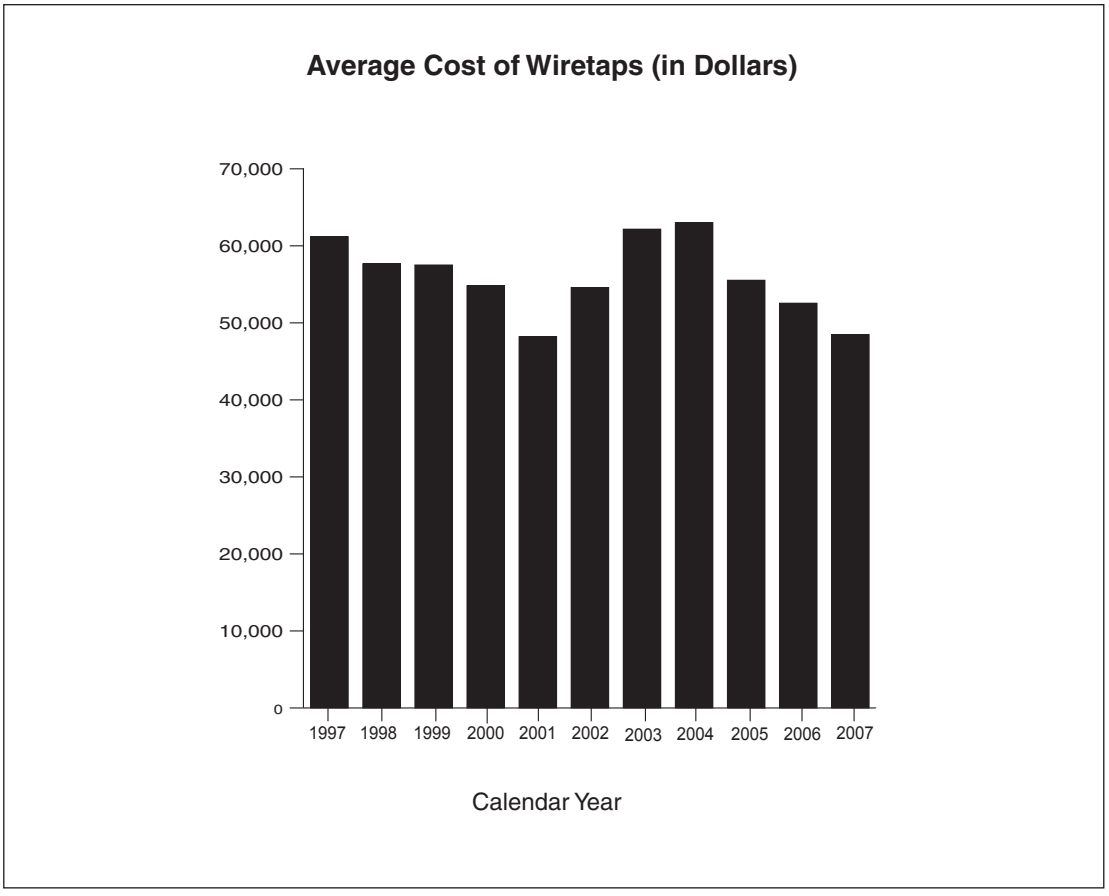
Table 6 presents the type of surveillance method used for each intercept installed. The most common method of surveillance reported was "phone wire communication," which includes all telephones (land line, cellular, cordless, and mobile). Telephone wiretaps accounted for 94 percent (1,998 cases) of intercepts installed in 2007.

The next most common method of surveillance reported was the oral wiretap, including microphones. Oral wiretaps were used in 1 percent of intercepts (20 cases). The electronic wiretap, which includes devices such as digital display pagers, voice pagers, fax machines, and transmissions via computer such as electronic mail, accounted for less than 1 percent (15 cases) of intercepts installed in 2007; 9 of these involved computers, and 4 involved other electronic devices. A combination of surveillance methods was used in 4 percent of intercepts (86 cases); of these combination intercepts, 90 percent (78 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 2007, no instances were reported of encryption encountered during any federal or state wiretap.

Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 2007. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 2,043 authorizations for which reports included cost data. The average cost of intercept devices installed in 2007 was $48,477, down 7 percent from the average cost in 2006. For federal wiretaps for which expenses were reported in 2007, the average cost was $65,660, a 2 percent decrease from the average cost in 2006. The average cost of a state wiretap declined 7 percent to $43,584



in 2007. 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 2007. As of December 31, 2007, a total of 4,830 persons had been arrested based on interceptions of wire, oral, or electronic communications, 10 percent more than in 2006. Wiretaps terminated in 2007 resulted in the conviction of 984 persons as of December 31, 2007, which was 20 percent of the number of persons arrested. Federal wiretaps were responsible for 36 percent of the arrests and 24 percent of the convictions arising from wiretaps during 2007. The District of Colorado reported the most arrests arising from a wiretap terminated in 2007; a wiretap used in a narcotics investigation there yielded the arrest of 65 persons. A wiretap in Morris County, New Jersey, which resulted in the most arrests of any state intercept terminated in 2007, was the lead wiretap of 13 intercepts authorized for a narcotics investigation that led to the arrest of 105 persons. The leader among state intercepts in producing convictions was a wiretap authorized in Queens County, New York, for a narcotics investigation, which resulted in the conviction of 48 of the 51 persons arrested. The next-largest number of convictions reported to have stemmed from a state wiretap occurred in San Diego County, California, where the lead wiretap of 7 intercepts authorized in a narcotics investigation yielded the conviction of 47 persons. The District of Arizona reported the most convictions for any federal wiretap; there the lead wiretap of 9 intercepts authorized in a narcotics investigation produced convictions for all 26 persons arrested. A wiretap that was the lead wiretap of 3 used in a transport investigation in the District of Minnesota resulted in convictions for 18 of the 42 persons arrested.

Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. Surveillance of cellular telephone communications lasted 30 days during a money laundering investigation in the District of Nevada. The reporting official stated that this wiretap allowed identification of illegal activities and additional violations of law. The investigation has specifically targeted multiple sources, including an internet gambling business. Officials in the Western District of Missouri reported that cellular telephone surveillance identified several individuals who participated in the on-line procurement of drugs via internet pharmacies.

At the state level, the New York City Special Narcotics Bureau reported that a multi-state case, involving a cellular telephone wiretap, resulted in the seizure of 123 kilos of cocaine in Boston, Massachusetts, with the arrest of 5 individuals. In a separate narcotics investigation, the New York City Special Narcotics Bureau reported that 13 related cellular telephone wiretaps resulted in the seizure of $2.7 million and the indictment of 9 individuals. The District Attorney in Los Angeles, California, reported that interceptions obtained from a cellular telephone wiretap, conducted over 57 days in a narcotics investigation, resulted in the seizure of approximately 40 pounds of methamphetamine, 4 kilos of cocaine, $700,000, and the arrest of two persons.

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 2007 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, 1997 Through 2007

Table 7 provides information on intercepts reported each year from 1997 to 2007. 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 1997 to 2007, the number of intercept applications authorized, by year (as reported through 2007), increased 86 percent. The majority of wiretaps consistently have been used for drug crime investigations, which accounted for 81 percent of intercept applications in 2007. Be-

tween 1997 and 2007, the percentage of drug-related wiretaps ranged from 72 percent to 81 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 2007, a total of 1,883 arrests, 2,013 convictions, and additional costs of $23,880,074 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. Twenty-six percent of the supplemental reports of additional activity in 2007 involved wiretaps terminated in 2006. Of all supplemental arrests, convictions, and costs reported in 2007, intercepts concluded in 2006 led to 82 percent of arrests, 65 percent of convictions, and 87 percent of expenditures. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1997 through 2007.