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, 2008, and December 31, 2008, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 1,891 intercepts authorized by federal and state courts were completed in 2008, a decrease of 14 percent compared to the number terminated in 2007. The number of applications for orders by federal authorities fell 16 percent to 386. The number of applications reported by state prosecuting officials dropped 14 percent to 1,505, with 22 states providing reports, two fewer than in 2007. Installed wiretaps were in operation an average of 41 days per wiretap in 2008, compared to 44 days in 2007. The average number of persons whose communications were intercepted decreased from 94 per wiretap order in 2007 to 92 per wiretap order in 2008. The average percentage of intercepted communications that were incriminating was 19 percent in 2008, compared to 30 percent in 2007.

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 2008, two instances were reported of encryptions encountered during state wiretaps; neither prevented officials from obtaining the plain text of the communications.

The appendix tables of this report list all intercepts reported by judges and prosecuting officials for 2008. 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 2008 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 54 state and local prosecutors' reports were missing in 2008, compared to 56 in 2007. 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 2009

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 2008, a total of 23 jurisdictions reported using at least one of these three types of surveillance as an investigative tool.

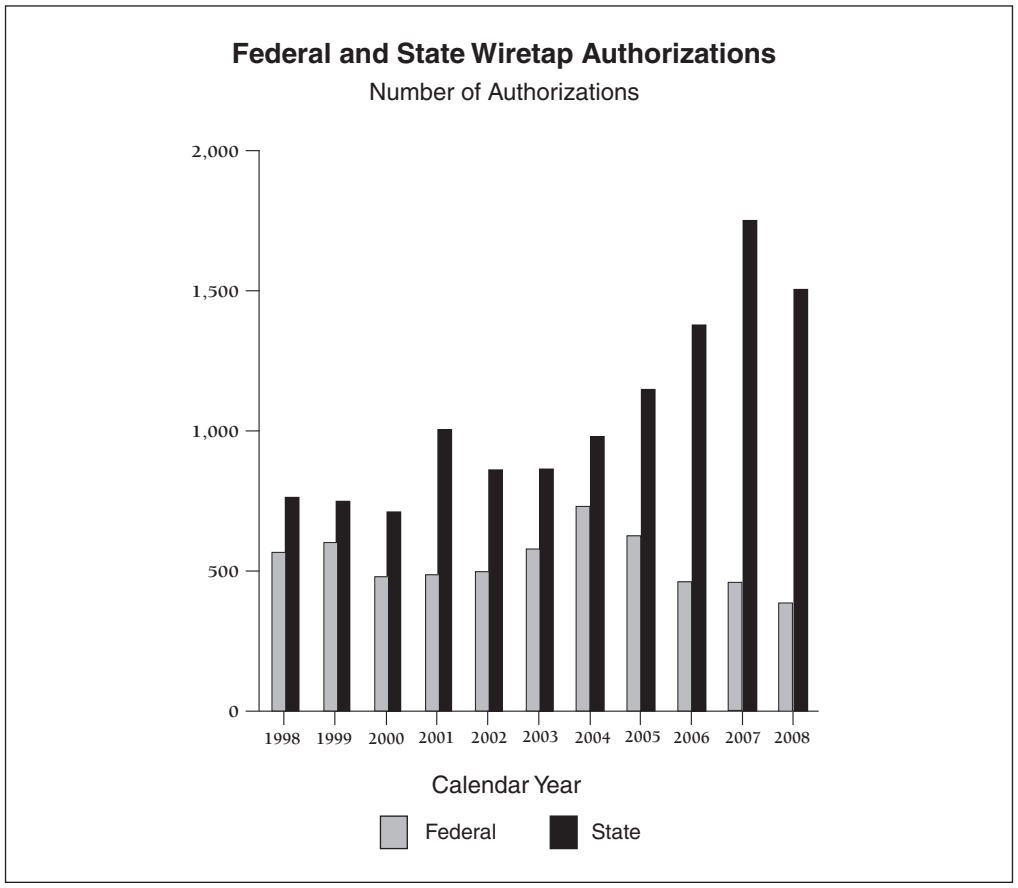
Summary and Analysis of Reports by Judges

Data on applications for wiretaps terminated during calendar year 2008 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 decreased 14 percent in 2008. A total of 1,891 applications were reported as authorized in 2008, including 386 submitted to federal judges and 1,505 to state judges. No applications were denied. Compared to the number approved during 2007, the number of applications reported as approved by federal judges in 2008 fell 16 percent. The number of applications approved by state judges declined 14 percent. Wiretap applications in New York (433 applications), California (418 applications), New Jersey (175 applications), and Florida (102 applications) accounted for 75 percent of all applications approved by state judges. The number of states reporting wiretap activity was lower than the number for last year (22 states reported such activity in 2008, compared to 24 in 2007). In 2008, a total of 110 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, which is 7 fewer than the total for 2007.

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 2008, the average length of an original authorization was 29 days, the same average length as in 2007. A total of 1,266 extensions were requested and authorized in 2008, a decrease of 26 percent. The average length of an extension remained unchanged at 29 days. The longest federal intercepts occurred in two districts, the Central District of California and the Southern District of Texas, where the original 30-day orders were extended 6 times in each district to complete 2 wiretaps lasting 210 days that were used in racketeering and narcotics investigations, respectively. Among state wiretaps terminating during 2008, the longest was used in a narcotics investigation conducted by the New York Organized Crime Task Force; this wiretap, in use for 590 days, required the original order to be extended 20 times. In contrast, 12 federal intercepts and 70 state intercepts were in operation for less than a week.

Locations

The most common location specified in wiretap applications authorized in 2008 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 2008, a total of 95 percent (1,793 wiretaps) of all intercepts authorized involved portable devices such as these, which are not limited to fixed locations. This is a slight increase from 2007, when 94 percent of all intercepts involved portable devices.

The next most common location reported for the placement of wiretaps in 2008 was a combination of locations, which was noted in 38 applications (2 percent of the total). The category "personal residence," a type of location that includes single-family houses as well as row houses, apartments, and other multi-family dwellings, was the third most common location cited. Table 2 shows that in 2008, almost 2 percent of all intercept devices (31 wiretaps) were authorized for personal residences. Ten wiretaps were authorized for "other" locations, which included such places as prisons, pay telephones in public areas, and motor vehicles. Six wiretaps were authorized for business establishments such as offices, restaurants, and hotels. Together, "other" and business establishments accounted for less than 1 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" (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 2008, authorizations for 11 wiretaps indicated approval with a relaxed specification order, meaning they were considered roving wiretaps. This is a decrease from 2007, when 21 wiretaps were reported as roving wiretaps. All 11 roving wiretaps were reported by state authorities: 6 were used in racketeering investigations, and 5 in a narcotics investigations.

Offenses

Violations of drug laws and homicide/assault were the two most prevalent types of offenses investi-

gated through communications intercepts. Racketeering was the third most frequently recorded offense category, and gambling the fourth. Table 3 indicates that 84 percent of all applications for intercepts (1,593 wiretaps) authorized in 2008 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 Central District of California (33 applications), the Southern District of New York (30 applications), and the Southern District of Texas (21 applications). On the state level, the largest numbers of drug-related intercepts were reported by Los Angeles County of California (164 applications), Queens County of New York (118 applications), and the New York City Special Narcotics Bureau (101 applications). Nationwide, homicide/assault was specified in 5 percent of applications (92 orders) as the most serious offense under investigation. Racketeering was specified in 3 percent of applications (58 orders) as the most serious offense under investigation. The category of gambling was specified in almost 3 percent of applications (54 orders). One other offense category in Table 3 with a significant total was larceny (43 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 2008. Judges submitted 54 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*.

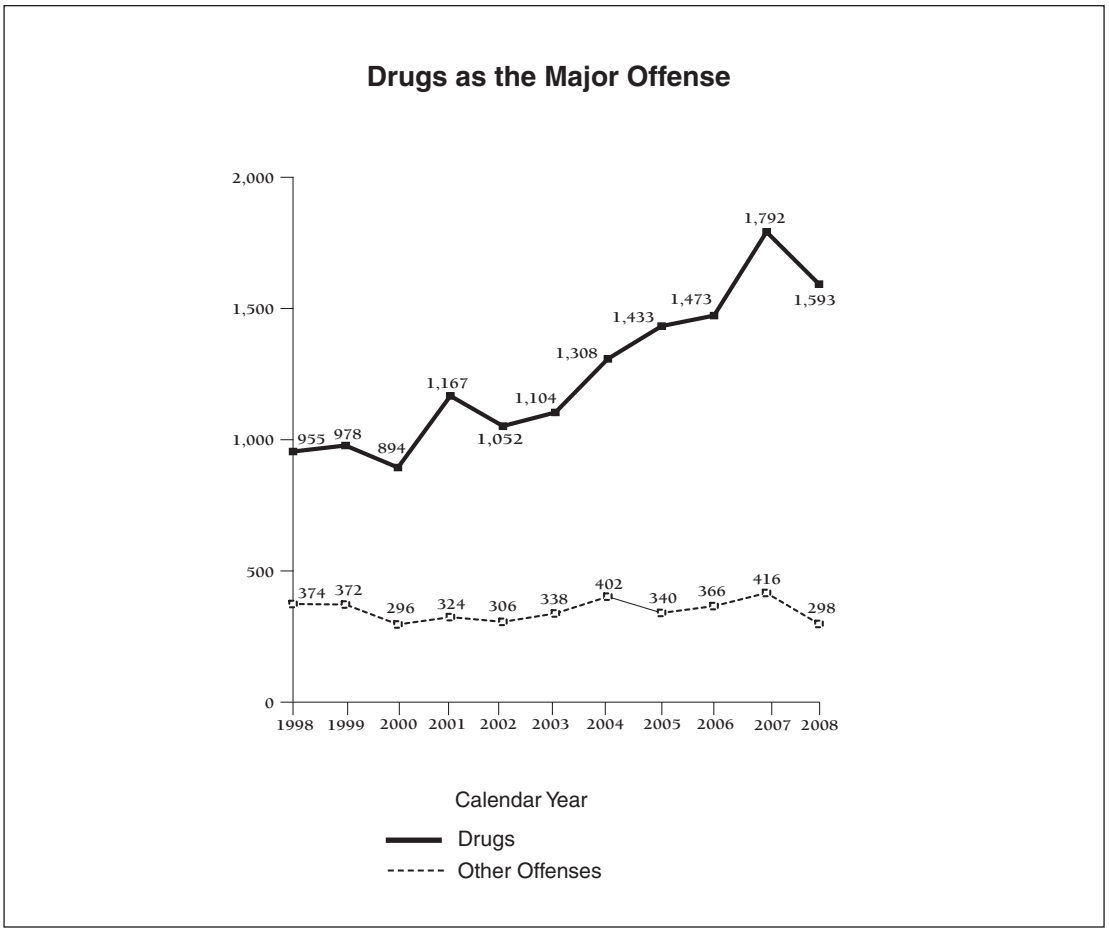
Nature of Intercepts

Of the 1,891 communication interceptions authorized in 2008, reports submitted by prosecutors indicated that intercept devices were installed and results were reported in conjunction with a total of 1,809 orders. As shown in Table 2, orders for 28 wiretaps were approved for which no wiretaps actually were installed, and results from 54 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 2008, installed wiretaps were in operation an average of 41 days, 3 days fewer than the average number of days wiretaps were in operation in 2007. Three interrelated federal wiretaps with the most intercepts occurred in the Northern District of Illinois, where narcotics investigations involving cellular telephones and other electronic communications resulted in the interception of 104,777 messages. The federal wiretap with the second highest number of intercepts, a cellular telephone wiretap, occurred in the Southern District of California as part of a narcotics investigation; this wiretap was active for 60 days and resulted in a total of 33,419 interceptions.

The state wiretap with the most intercepts was conducted by the New York Organized Crime Task Force, which used a 590-day wiretap in a narcotics investigation involving cellular telephones and oral communications that resulted in the interception of 168,292 messages, 18,353 of which were incriminating. A second wiretap installed by the New York Organized Crime Task Force lasted 219 days and generated a total of 58,926 cellular and standard telephone intercepts.

Nationwide, in 2008 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 2,707 per wiretap. An average of 514 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order decreased from 30 percent in 2007 to 19 percent in 2008.



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 97 percent (1,757 cases) of intercepts installed in 2008.

The next most common method reported was a combination of surveillance devices, which usually includes a mobile/cellular telephone with another type of oral or electronic device. Combined wiretaps were used in 2 percent of intercepts (33 cases). In 2008, a combination intercept reported for Middlesex County in Massachusetts included cellular and standard telephones, a microphone, and a fax machine. The electronic wiretap, which includes digital display pagers, voice pagers, fax machines, and transmissions via computer such as electronic mail, accounted for less than 1 percent (10 cases) of intercepts installed in 2008.

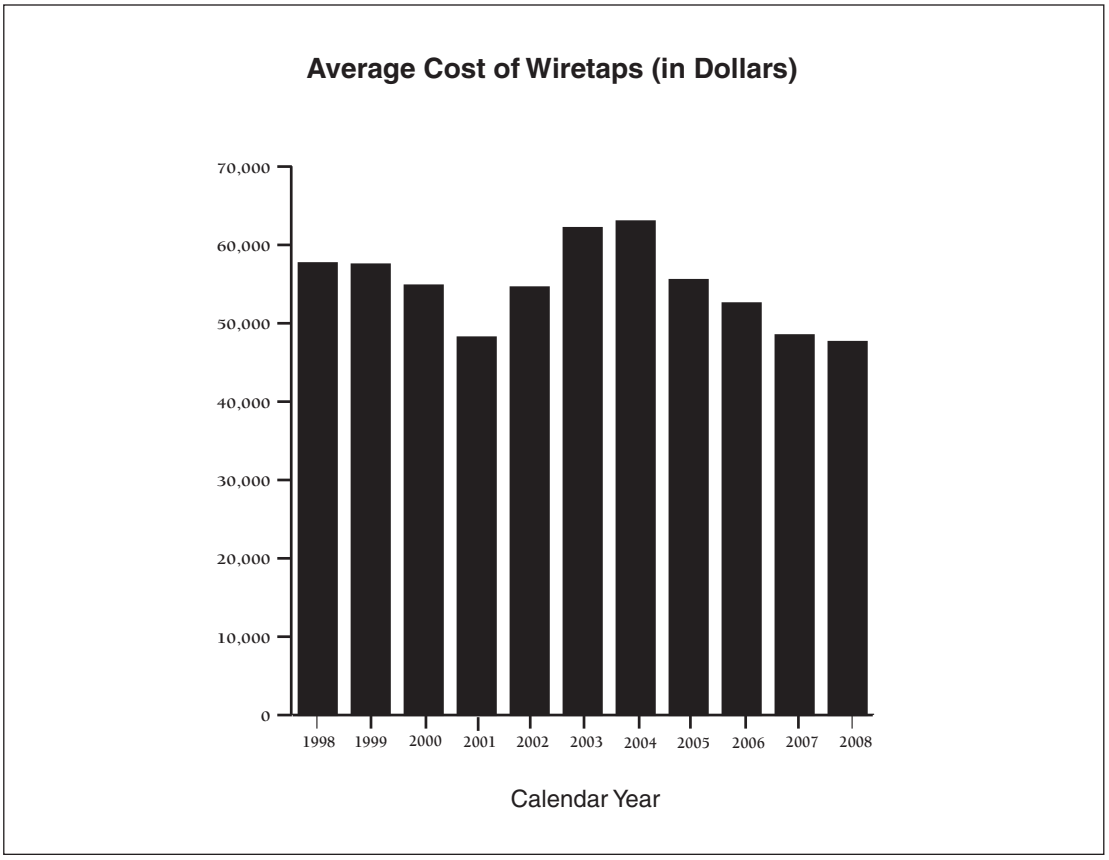
Public Law 106-197 amended 18 U.S.C. 2519(2)(b) in 2001 to require that reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2008, encryption was encountered during two state wiretaps; neither instance prevented officials from obtaining the plain text of the communications.

Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 2008. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,703 authorizations for which reports included cost data. The average cost of intercept devices installed in 2008 was $47,624, down 2 percent from the average cost in 2007. For federal wiretaps for which expenses were reported in 2008, the average cost was $70,536, a 7 percent increase from the average cost in 2007. The average cost of a state wiretap declined 6 percent to $41,154 in 2008. 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 2008. As of December 31, 2008, a total of 4,133 persons had been arrested based on interceptions of wire, oral, or electronic communications, 14 percent fewer than in 2007. Wiretaps terminated in 2008 resulted in the conviction of 810 persons as of December 31, 2008, which was 20 percent of the number of persons arrested. Federal wiretaps were responsible for 38 percent of the arrests and 29 percent of the convictions arising from wiretaps during 2008. The Central District of California reported the most arrests arising from a federal wiretap terminated in 2008; seven related wiretaps in a racketeering investigation there yielded the arrest of 118 persons. A wiretap in Maricopa County, Arizona, which caused the most arrests of any state intercept terminated in 2008, led to arrest of 65 persons in connection with a narcotics investigation. The leader among state intercepts in producing convictions was a wiretap authorized in the 11th Judicial District (Hamilton), Tennessee, for a narcotics investigation, which resulted in the conviction of 40 of the 43 persons arrested. The next-largest number of convictions reported to have stemmed from a state wiretap occurred in Queens County, New York, where the lead wiretap of 50 intercept orders authorized in a theft investigation yielded the conviction of 33 persons. The Southern District of Ohio reported the most convictions for any federal wiretap; there the lead wiretap of 2 intercepts authorized in a narcotics investigation produced convictions for 30 of the 31 persons arrested.



Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. Speaking of a 60-day surveillance of cellular telephone communications during a federal narcotics investigation in the Northern District of Texas, the reporting official stated that this wiretap allowed identification of illegal activities that resulted in the arrest of 17 individuals and the seizure of 370 kilos of cocaine, 360 pounds of methamphetamine, 20 weapons, 5 vehicles, and $8 million in cash. In the Eastern District of Virginia, a routine federal narcotics surveillance identified incriminating cellular telephone communications that led to the arrest of 16 individuals and conviction of 10, as well as the seizure of $2.3 million, 7 weapons, and 2 vehicles.

At the state level, San Diego County reported that a multi-jurisdiction case involving a cellular telephone wiretap resulted in the seizure of 52 kilos of cocaine and $2 million, along with the arrest of 47 individuals and the conviction of 25. The New York City Special Narcotics Bureau reported that a cellular telephone wiretap led to the seizure of 180 kilos of cocaine and $400,000. In a separate narcotics investigation, the New York City Special Narcotics Bureau reported that interceptions obtained from a cellular telephone wiretap conducted over 36 days in a narcotics investigation resulted in the seizure of approximately 30 kilos of cocaine and $22,000.

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 2008 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, 1998 Through 2008

Table 7 provides information on intercepts reported each year from 1998 to 2008. 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 1998 to 2008, the number of intercept applications authorized by year (as reported through 2008) increased 42 percent. The majority of wiretaps consistently have been used for drug crime investigations, which accounted for 84 percent of intercept applications in 2008. Between 1998 and 2008, the percentage of drug-related wiretaps ranged from 72 percent to 84 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 2008, a total of 3,311 arrests, 2,698 convictions, and additional costs of $31,076,214 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-six percent of the supplemental reports of additional activity in 2008 involved wiretaps terminated in 2007. Of all supplemental arrests, convictions, and costs reported in 2008, intercepts concluded in 2007 led to 52 percent of arrests, 44 percent of convictions, and 72 percent of expenditures. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1998 through 2008. ■