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, 2009, and December 31, 2009, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 2,376 intercepts authorized by federal and state courts were completed in 2009. The number of applications for orders by federal authorities was 663. The number of applications reported by state prosecuting officials was 1,713, with 24 states providing reports, two more than in 2008. Installed wiretaps were in operation an average of 42 days per wiretap in 2009, compared to 41 days in 2008. The average number of persons whose communications were intercepted rose from 92 per wiretap order in 2008 to 113 per wiretap order in 2009. The average percentage of intercepted communications that were incriminating remained unchanged at 19 percent in 2009.

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 2009, one instance was reported of encryption encountered during a state wiretap; however, this did not prevent 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 2009. 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 2009 arising from intercepts initially reported in prior years.

Title 18 U.S.C. § 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 324 federal prosecutors' reports and 252 state and local prosecutors' reports were missing in 2009. 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 2010

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 separate written report with the Director of the Administrative Office of the United States Courts (AO) on each application for a court 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 expiration of the court order (after all extensions have expired) or within 30 days after the denial of the application. The report must include the name of the prosecuting official who applied for the order, the criminal offense under investigation, the type of interception device, the physical location of the device, and the duration of the intercept.

Prosecuting officials who applied for interception orders, including the Attorney General of the United States or his or her designee at the federal level and any prosecuting attorneys with statutory authority at the state level, are required to submit reports to the AO in January on all orders that expired during the previous calendar year. These reports contain information related to the cost of the intercept, the number of days the intercept device was in operation, the total number of intercepts, and the number of incriminating intercepts recorded. Results of the interception orders such as arrests, trials, convictions, and the number of motions to suppress evidence also are noted in these reports. However, neither the judges' reports nor the prosecuting officials' reports include the names, addresses, or phone numbers of parties investigated. The AO is **not** authorized by statute to collect this information.

This document 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 devices were installed, as reported by prosecuting officials. No statistics are collected on the number of devices used in conjunction with each order. This document does not reflect interceptions regulated by the Foreign Intelligence Surveillance Act of 1978 (FISA).

No report to the AO is needed when an order is issued with the consent of one of the principal parties to the communication. 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 recorded.

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 wiretap statute may be obtained by writing to the Administrative Office of the United States Courts, Statistics Division, Washington, DC, 20544.

Table 1 reveals 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 2009, a total of 24 jurisdictions reported using at least one of these types of surveillance as an investigative tool.

Summary and Analysis of Reports by Judges

Data on applications for wiretaps terminated during calendar year 2009 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 AO-assigned reporting number is required for any supplemental information submitted for an intercept that appears in subsequent volumes of the *Wiretap Report*.

The number of federal and state wiretaps reported in 2009 increased 26 percent. A total of 2,376 were reported as authorized in 2009, with 663 authorized by federal judges and 1,713 authorized by state judges. No applications were denied. This

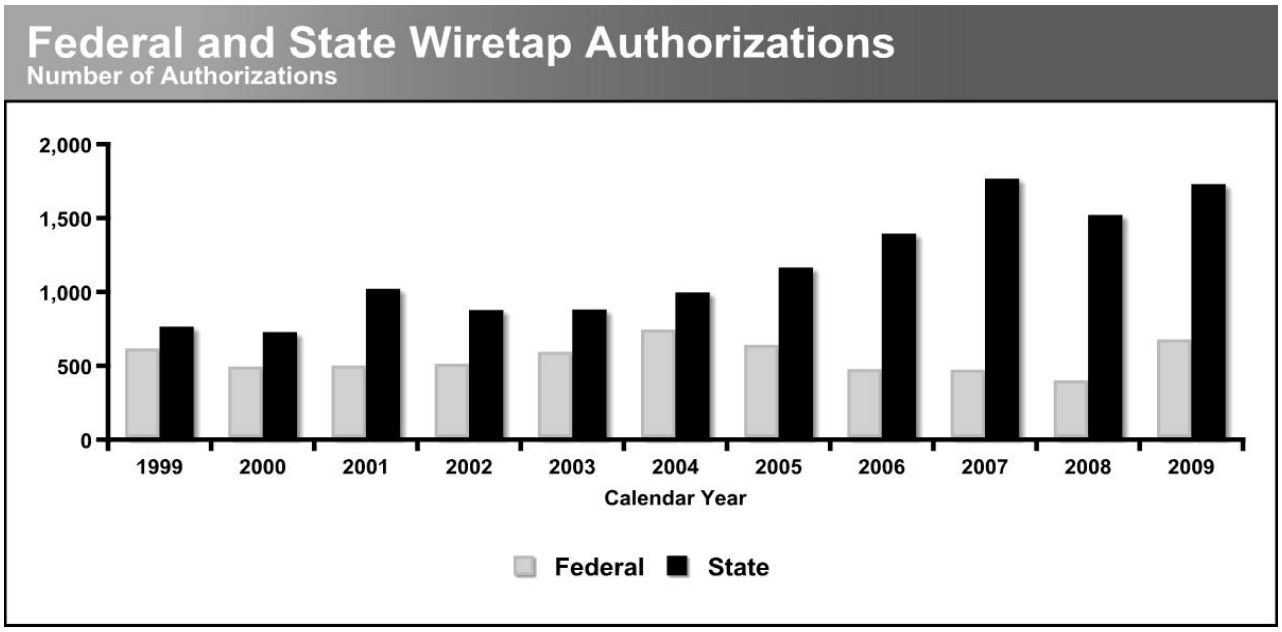
States with Largest Numbers of Applications Approved by State Judges		
State	**Number of Applications**	**Percent of Total**
California	586	34
New York	424	25
New Jersey	206	12

increase was due, at least in part, to enhanced AO efforts to ensure that federal and state authorities were aware of their wiretap reporting responsibilities under 18 U.S.C. § 2519(1). Compared to the number approved during 2008, the number of applications reported as approved by federal judges rose 72 percent in 2009. The number of applications approved by state judges increased 14 percent. Wiretap applications in California, New York, and New Jersey accounted for 71 percent of all applications approved by state judges (see table below). In 2009, a total of 108 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, compared to 110 in 2008.

Intercept Orders, Extensions, and Locations

Table 2 presents the number of intercept orders issued in each jurisdiction that provided reports, the number of extensions granted, the average lengths of the original periods authorized and any extensions, the total number of days in operation, and the locations of the communications intercepted. 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 is justified.

During 2009, the average length of an original authorization was 29 days, the same average length as in 2008. A total of 1,627 extensions were requested and authorized in 2009, an increase of 29 percent. The average length of an extension was 28 days. For federal intercepts terminated in 2009, the longest intercept occurred in the District of Nevada, where the original order was extended four times to complete a 139-day wiretap used in a narcotics investigation. Reports for two other federal wiretaps that were submitted in 2009



for previous reporting periods, one for the Eastern District of Michigan and one for the Southern District of New York, were extended 300 days and 330 days, respectively. The longest state wiretap, which was used in a corruption investigation conducted by the New York Organized Crime Task Force, was in use for a total of 632 days. The second-longest state wiretap was used in a gambling investigation orchestrated by Queens County, New York, for a total of 615 days.

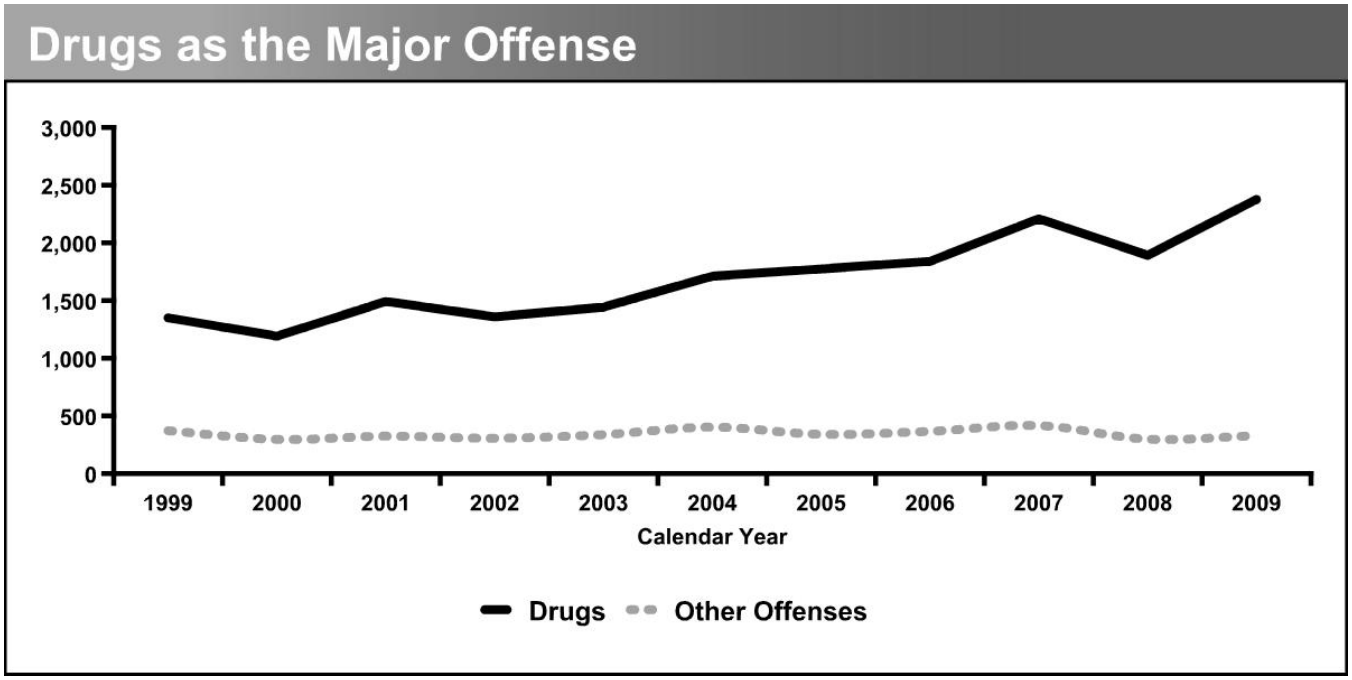
The most frequently noted location in wiretap applications was "portable device," a category that includes cellular telephones and digital pagers. In recent years, the number of wiretaps involving fixed locations has declined as the use of mobile communications, including text messaging from cellular telephones, has become increasingly widespread. In 2009, a total of 96 percent (2,276 wiretaps) of all authorized wiretaps were designated as portable devices.

The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2518(11)) and the Intelligence Authorization Act of 1999 (18 U.S.C. § 2518(11)(b)) provide that prosecutors, upon showing probable cause to believe that the party being investigated is avoiding intercepts at a particular site, may use relaxed specification or "roving" wiretaps to target specific persons by using electronic devices at multiple locations rather than a specific telephone or location. For 2009, no federal wiretaps were designated as roving. Sixteen state authorizations were approved as roving wiretaps, most of which also involved other types of locations.

Criminal Offenses

Drug crimes were the most prevalent type of criminal offenses investigated using wiretaps. Homicide was the second most frequently cited crime, followed by other major offenses and racketeering. Table 3 indicates that 86 percent of all applications for intercepts (2,046 wiretaps) in 2009 cited illegal drugs as the most serious offense under investigation. Many applications for court orders revealed that multiple criminal offenses were under investigation, but Table 3 includes only the most serious criminal offense listed on the application.

Many wiretaps were requested to conduct federal drug investigations in the District of Arizona (62 applications), the Northern District of Illinois (45 applications), and the Southern District of Texas (37 applications). On the state level, the largest numbers of drug-related wiretaps were reported by Los Angeles County of California (166 applications), San Bernardino County of California (118 applications), and the New York City Special Narcotics Bureau (111 applications). Nationally, homicide was specified as



the most serious offense in 4 percent of applications; other major offenses and racketeering were specified in less than 3 percent.

Summary of Analysis and Reports by Prosecuting Officials

Pursuant to 18 U.S.C. § 2519(2), prosecuting officials must submit reports to the AO no later than January 31 of each year for wiretaps terminated during the previous calendar year. Appendix Tables A-1 and B-1 contain information from all prosecutors' reports submitted for 2009. Federal and state judges submitted 324 reports and 252 reports, respectively, for which the AO received no corresponding reports from prosecuting officials. Table 10 shows the total number of intercept orders authorized by federal judges by jurisdiction through December 31, 2009. For state authorizations, the entry "NP" (no prosecutor's report) appears in the appendix tables. Some of the prosecutors' reports were received too late to include in this document, and some prosecutors delayed filing reports to avoid jeopardizing ongoing investigations; information from these reports will appear in future volumes of the *Wiretap Report*.

Lengths and Numbers of Intercepts

In 2009, installed wiretaps were in operation for an average of 42 days, 1 day more than the average number of days wiretaps were in operation in 2008. The federal wiretap with the most intercepts occurred in the District of Arizona, where a narcotics investigation involving cellular telephones resulted in the interception of 31,062 messages over 71 days. The second-highest number of intercepts stemmed from a cellular telephone wiretap in the District of Wyoming for a narcotics investigation; this wiretap was active for 87 days and resulted in a total of 30,008 interceptions.

The state wiretap with the most intercepts was conducted in New York County, New York, where a 543-day wiretap in a corruption investigation involved various types of interceptions, including text messaging, and resulted in the interception of 322,000 messages, 11,000 of them incriminating. A wiretap installed by the New York Organized Crime Task Force lasted 266 days and generated 149,313 cellular telephone, microphone, and electronic interceptions.

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 the communications intercepted pursuant to the court orders. In 2009, encryption was encountered during one state wiretap, but did not prevent officials from obtaining the plain text of the communications.

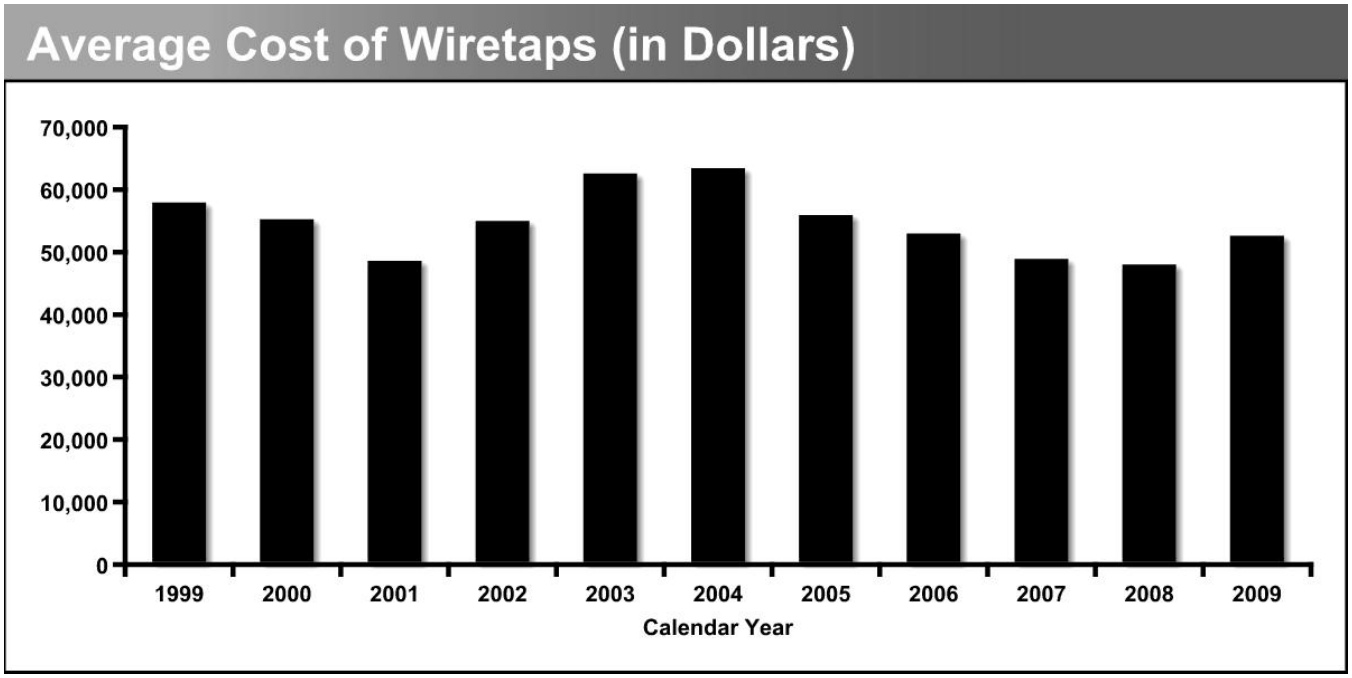
Costs of Intercepts

Table 5 provides a summary of expenses related to wiretaps in 2009. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,564 authorizations for which reports included cost data. The average cost of intercept devices in 2009 was $52,200, up 10 percent from the average cost in 2008. For federal wiretaps for which expenses were reported in 2009, the average cost was $62,552, an 11 percent decrease from the average cost in 2008. The cost of a state wiretap ranged from a low of $700 in Columbia County, Pennsylvania, to a high of $541,124 for investigations by the New York Organized Crime Task Force.

Methods of Surveillance

The three major categories of surveillance are wire, oral, and electronic communications. For many years, nearly all intercepts involved telephone (wire) surveillance, primarily communications made via conventional telephone lines; the remainder involved microphone (oral) surveillance. A third category was added for reporting electronic communications with the passage of the Electronic Communications Privacy Act of 1986. These communications usually are made through digital-display paging devices, fax machines, text messaging, and computer transmissions.

Table 6 presents the type of surveillance method used for each intercept installed. The most common method reported was wire surveillance that used a telephone (land line, cellular, cordless, or mobile).



Telephone wiretaps accounted for 98 percent (1,720 cases) of the intercepts installed in 2009, the majority of them involving cellular telephones.

Arrests and Convictions

Data on individuals arrested and convicted as a result of interceptions reported as terminated are presented in Table 6. As of December 31, 2009, a total of 4,537 persons had been arrested (up 10 percent from 2008), and 678 persons had been convicted (down 16 percent from 2008). Federal wiretaps were responsible for 28 percent of the arrests and 18 percent of the convictions arising from wiretaps for this period. The Southern District of California reported the most arrests for a wiretap originally authorized in 2007; a wiretap used in a narcotics investigation in that district yielded the arrest of 170 individuals with 17 convictions. A narcotics investigation in the District of Arizona for 2008 resulted in the arrest of 169 individuals with 116 convictions. The table below presents the three state wiretaps for which the most arrests were reported.

Federal and state prosecutors often note the importance of wiretap surveillance in obtaining arrests and convictions. A wiretap in a federal narcotics investigation in the Southern District of Florida uncovered incriminating cellular telephone communications that led to the arrests of 45 individuals and the seizure of 10 kilos of cocaine, $166,000 in cash, 10 weapons, and 14 vehicles. In the District of Arizona, the reporting officials stated that a narcotics investigation identified illegal activity that resulted in the arrests of four individuals and the seizure of 3,827 pounds of

State Wiretaps Resulting in the Most Arrests

County and State	Type of Offense	Number of Arrests
Maricopa County, AZ	Narcotics	130
Maricopa County, AZ	Narcotics	110
Gwinnett County, GA	Narcotics	80

marijuana, four vehicles, and one weapon. At the state level, the Second Judicial District (Denver) in Colorado reported that a cellular telephone wiretap resulted in the seizure of 1,300 grams of cocaine, 800 grams of methamphetamine, and 1,700 grams of marijuana and firearms, along with the arrests of nine persons and the convictions of six.

Summary of Reports for Years Ending December 31, 1999 Through 2009

Table 7 presents data on intercepts reported each year from 1999 to 2009. The number of intercept applications authorized by year increased 76 percent between 1999 and 2009. The majority of the wiretaps consistently have been used for drug crime investigations, which accounted for 72 percent of intercepts in 1999 (978 applications) and 86 percent (2,046 applications) in 2009. Table 9 presents the total numbers of arrests and convictions resulting from intercepts terminated in calendar years 1999 through 2009.

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, supplemental 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 an intercept was first reported. Appendix Tables A-2 (Federal) and B-2 (State) provide detailed data from the supplementary reports submitted.

During 2009, a total of 4,269 arrests, 2,830 convictions, and additional costs of $47,039,345 arose from and were reported for wiretaps completed in previous years. Sixty-five percent of the supplemental reports of additional activity in 2009 involved wiretaps terminated in 2008. Interceptions concluded in 2008 led to 60 percent of arrests, 51 percent of convictions, and 68 percent of expenditures noted in the supplementary reports.