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, 2010, and December 31, 2010, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

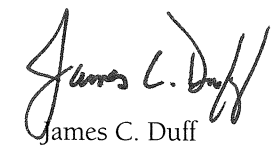
A total of 3,194 intercepts authorized by federal and state courts were completed in 2010, an increase of 34 percent compared to the number reported in 2009. The number of applications for orders reported by federal authorities was 1,207. The number of applications reported by state prosecuting officials was 1,987, with 25 states providing reports. Installed wiretaps were in operation an average of 40 days per wiretap in 2010, compared to 42 days in 2009. The average number of persons whose communications were intercepted rose from 113 per wiretap order in 2009 to 118 per wiretap order in 2010. Twenty-six percent of intercepted communications in 2010 were incriminating.

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 2010, six instances were 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 2010. 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 2010 arising from intercepts initially reported in prior years.

Public Law 111-174 amended 18 U.S.C. § 2519 to change the deadlines for federal and state judges to submit reports to the AO on approved or denied orders for wiretaps and for prosecutors to submit data to the AO on wiretap orders. Judges now must submit reports to the AO by January 31 on all wiretap orders they acted on during the previous calendar year. Prosecutors now must submit reports to the AO by March 31 on wiretap orders they applied for during the previous calendar year. In addition, the Director of the AO now must submit this annual report of wiretap activity to Congress in June.

This office, as is customary, sends a letter to the appropriate officials every year reminding them of the statutory mandate to report wiretap data. 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 566 federal prosecutors' reports and 267 state and local prosecutors' reports on wiretap activity in 2010 were not submitted. 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

June 2011

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)). The reports for all wiretap orders must be submitted to the AO by January 31 of the subsequent year after expiration of the court order (after all extensions have expired) or 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 by March 31 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 are also noted in these reports. Neither the judges' reports nor the prosecuting officials' reports, however, 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.

On May 27, 2010, Public Law 111-174 adjusted the deadlines for the submission of wiretap reports. Previously, 18 U.S.C. § 2519(1) required federal and state judges to submit reports to the AO no later than 30 days after the expiration of an approved order or the denial of an order for a wiretap, and 18 U.S.C. § 2519(2) required prosecutors to submit information to the AO no later than January on wiretap orders they had applied for during the preceding calendar year. According to the amended provisions of 18 U.S.C. § 2519, judges must now submit reports to the AO no later than January 31 on all wiretap orders they acted on during the previous calendar year, and prosecutors must submit reports to the AO on wiretap orders applied for during the previous calendar year no later than March 31. In addition, the statute now provides that the Director of the AO shall submit this annual report of wiretap activity to Congress in June (previously, this report was due to Congress in April).

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 2010, a total of 26 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 2010 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 2010 increased 34 percent. A total of 3,194 wiretaps were reported as authorized in 2010, with 1,207 authorized by federal judges and 1,987 authorized by state judges. One application was denied. Compared to the numbers approved during 2009, the number of applications reported as approved by federal judges rose 82 percent in 2010, and the number of applications approved by state judges increased 16 percent. These increases were due, at least in part, to enhanced AO efforts to ensure that federal and state authorities were aware of their reporting responsibilities under 18 U.S.C. § 2519. In August 2009, the AO revised the wiretap form by separating Part 1 (completed by judges) from Part 2 (completed by federal or state prosecutors) of the form. This enabled judges to submit Part 1 of the wiretap form independently of Part 2, thereby enhancing the accuracy of the AO reports. The impact of the form revision was reflected to some degree in the *2009 Wiretap Report*, but is reflected more fully in this *2010 Wiretap Report*.

Wiretap applications in California, New York, and New Jersey accounted for 68 percent of all applications approved by state judges (see table below). In 2010, a total of 106 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, compared to 108 in 2009.

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 2010, the average length of an original authorization was 29 days, the same average length as in 2009. In total, 1,925 extensions were requested and authorized in 2010, an increase of 18 percent. The average length of an extension was 29 days. For federal intercepts terminated in 2010, the longest intercept occurred in the Southern District of California, where the original order was extended six times to complete a 210-day wiretap used in a narcotics investigation. A report for another federal wiretap that was submitted in 2010 for a previous reporting period indicated that an order in the District of Alaska was extended 330 days for a corruption investigation. The longest state wiretap, which was used in a narcotics investigation conducted by Queens County, New York, was employed for a total of 559 days. The second-longest state wiretap, which also was performed in Queens County, New York, was used in a corruption investigation for a total of 540 days.

The most frequently noted location in wiretap applications was "portable device," a category that includes

States With Largest Numbers of Applications Approved by State Judges

State	Number of Applications	Percent of Total
California	657	33
New York	480	24
New Jersey	215	11

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 2010, a total of 96 percent (3,053 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 2010, one federal wiretap was designated as roving. Seventeen state authorizations were approved as roving wiretaps.

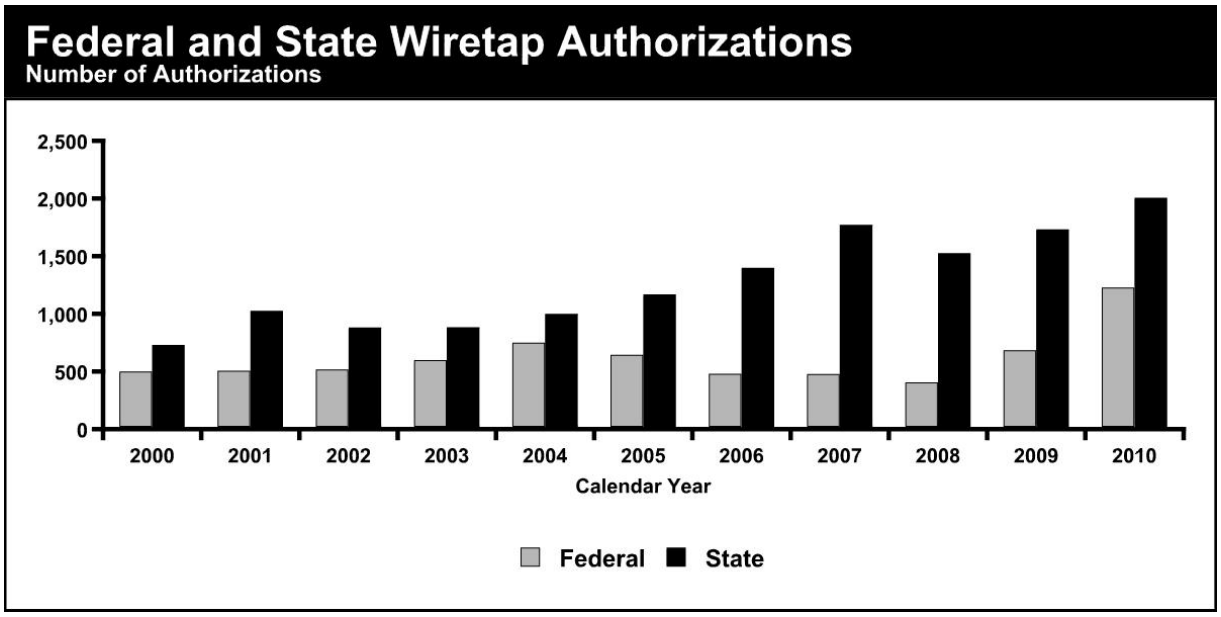
Criminal Offenses

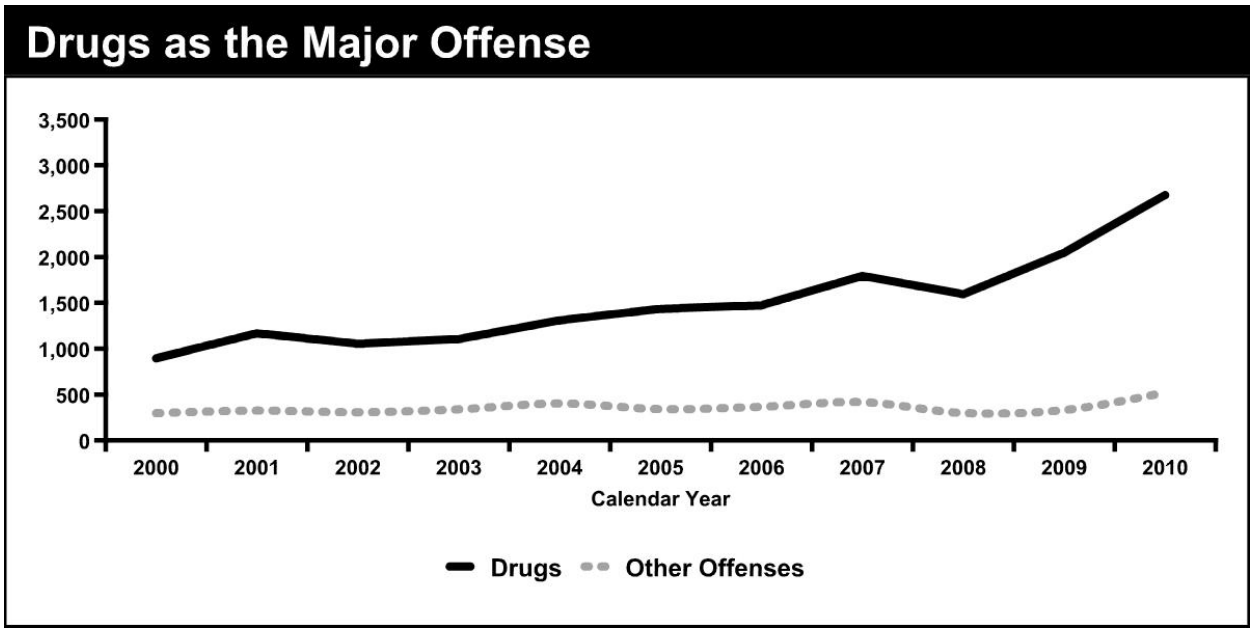
Drug offenses were the most prevalent type of criminal offenses investigated using wiretaps. Homicide was the second-most frequently cited crime, followed by racketeering. Table 3 indicates that 84 percent of all applications for intercepts (2,675 wiretaps) in 2010 cited illegal drugs as the most serious 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 Central District of California (61 applications), the Southern District of Texas (51 applications), and the Northern District of Illinois (42 applications). On the state level, the largest numbers of drug-related wiretaps were reported by Los Angeles County of California (182 applications), Queens County of New York (173 applications), and San Bernardino County of California (110 applications). Nationally, homicide was specified as the most serious offense in 5 percent of applications; racketeering was specified in less than 4 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 March 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 2010. Federal and state judges submitted 566 reports and 267 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, 2010. 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 should appear in future volumes of the *Wiretap Report*.

Lengths and Numbers of Intercepts

In 2010, installed wiretaps were in operation for an average of 40 days, 2 days less than in 2009. The federal wiretap with the most intercepts occurred in the Southern District of California, where a narcotics investigation involving cellular telephones resulted in the interception of 74,715 messages over 210 days. The second-highest number of intercepts stemmed from a cellular telephone wiretap in the Western District of Missouri for a narcotics investigation; this wiretap was active for 118 days and resulted in a total of 74,144 interceptions.

The state wiretap with the most intercepts was conducted in Queens County, New York, where a 62-day wiretap in a corruption investigation involving cell phone interceptions resulted in the interception of 134,410 messages. A wiretap installed in Gwinnett County, Georgia, lasted 415 days and generated 88,518 cellular telephone and text message 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 2010, encryption was reported during six state wiretaps, but did not prevent officials from obtaining the plain text of the communications.

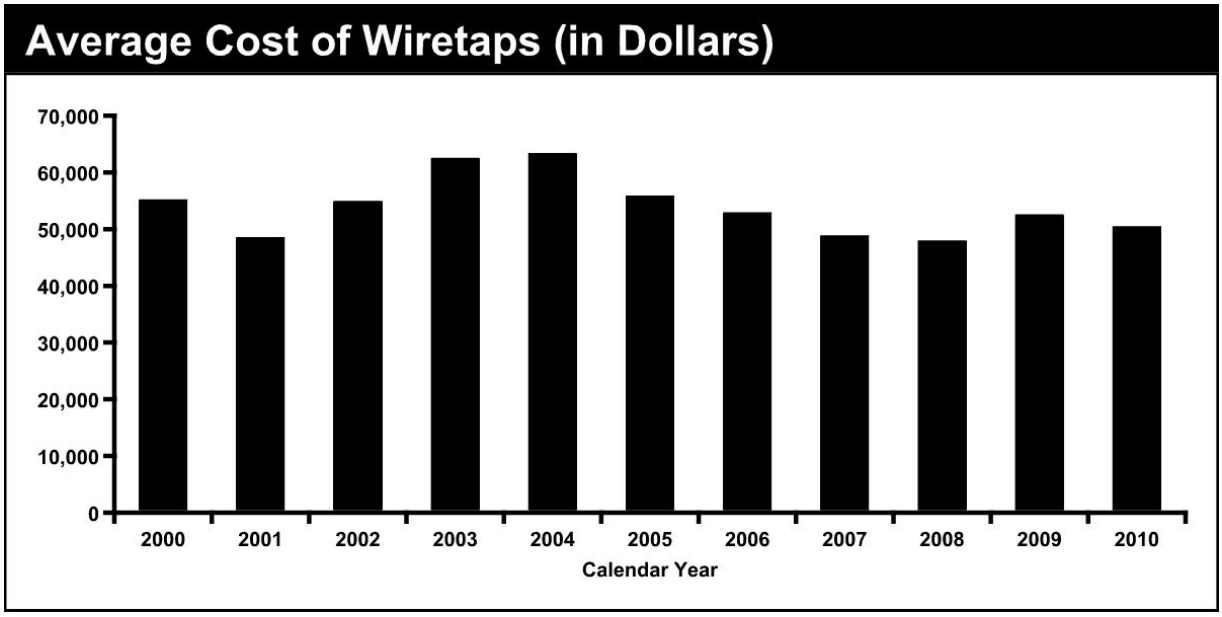
Costs of Intercepts

Table 5 provides a summary of expenses related to wiretaps in 2010. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 2,211 authorizations for which reports included cost data. The average cost of intercept devices in 2010 was $50,085, down 4 percent from the average cost in 2009. For federal wiretaps for which expenses were reported in 2010, the average cost was $63,566, a 2 percent increase from 2009. The cost of a state wiretap ranged from a low of $68 in Morris County, New Jersey, to a high of $1,697,030 for a murder investigation in Cape & Islands, Massachusetts.

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 97 percent (2,253 cases) of the intercepts installed in 2010, 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, 2010, a total of 4,711 persons had been arrested (up 4 percent from 2009), and 800 persons had been convicted (up 18 percent from 2009). Federal wiretaps were responsible for 48 percent of the arrests and 37 percent of the convictions arising from wiretaps for this period. The Southern District of Florida reported the most arrests for a wiretap; a wiretap used in a narcotics investigation in that district in 2010 yielded the arrest of 71 individuals with 35 convictions. A narcotics investigation in the District of Connecticut for 2009 resulted in the arrest of 52 individuals with 50 convictions. The table on page 11 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 Northern District of Georgia uncovered incriminating cellular telephone communications that led to the seizure of $3,304,711 in cash, 48 kilos of cocaine, 60 pounds of crystal methamphetamine, and 600 pounds of marijuana. In the Western District of Kentucky, the reporting officials stated that a narcotics investigation identified illegal activity that resulted in the arrests of 22 individuals and the seizure of $4,000,000 in cash, 13 vehicles, 16 firearms, 42 kilos of cocaine, and 3 pounds of marijuana. At the state level, a wiretap in a murder investigation in Los Angeles County, California, revealed "a series of approximately 3 murders, 9 attempted murders, and 4 shootings (11 separate incidents)" involving members of a gang. Several separate state jurisdictions reported that interceptions were instrumental for identifying and investigating sophisticated drug-trafficking organizations that were operating in the United States.

Summary of Reports for Years Ending December 31, 2000 Through 2010

Table 7 presents data on intercepts reported each year from 2000 to 2010. The number of authorized intercept applications reported by year increased 168 percent between 2000 and 2010. The majority of the wiretaps have consistently been used for drug crime investigations, which accounted for 75 percent of intercepts in 2000 (894 applications) and 84 percent (2,678 applications) in 2010. Table 9 presents the total numbers of arrests and convictions resulting from intercepts terminated in calendar years 2000 through 2010.

State Wiretaps Resulting in the Most Arrests		
County and State	**Type of Offense**	**Number of Arrests**
Marion County, IN	Narcotics	125
Queens, NY	Narcotics	90
Queens, NY	Narcotics	54

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 and B-2 provide detailed data from the supplementary reports submitted.

During 2010, a total of 2,852 arrests, 2,504 convictions, and additional costs of $39,259,171 arose from and were reported for wiretaps completed in previous years. Seventy percent of the supplemental reports of additional activity in 2010 involved wiretaps terminated in 2009. Interceptions concluded in 2009 led to 66 percent of arrests, 49 percent of convictions, and 82 percent of expenditures noted in the supplementary reports.