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, 2011, and December 31, 2011, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

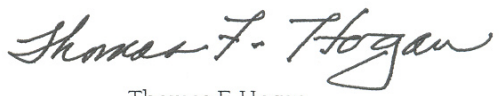
After rising 34 percent the previous year, the total number of intercepts authorized by federal and state courts and completed in 2011 decreased 14 percent to 2,732. The number of applications for orders reported by federal authorities was 792. The number of applications reported by state prosecuting officials was 1,940, with 25 states providing reports. Installed wiretaps were in operation an average of 42 days per wiretap in 2011, compared to 40 days in 2010. The average number of persons whose communications were intercepted decreased from 118 per wiretap order in 2010 to 113 per wiretap order in 2011. Twenty-three percent of intercepted communications in 2011 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. Twelve instances were reported of encryption encountered during state wiretaps in 2011; 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 2011. 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 2011 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 423 federal prosecutors' reports and 67 state and local prosecutors' reports on wiretap activity in 2011 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.



Thomas F. Hogan
Director

June 2012

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 (18 U.S.C. § 2519(2)). 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. 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. To see the wiretap reports, go to http://www.uscourts.gov/Statistics/WiretapReports.aspx. To obtain the reporting forms, go to http://www.uscourts.gov/FormsAndFees/Forms/CourtForms.aspx.

Table 1 lists the 48 jurisdictions (the federal government, the District of Columbia, the Virgin Islands, Puerto Rico, and 44 states) that currently have laws authorizing courts to issue orders permitting wire, oral, or electronic surveillance. For 2011, 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 2011 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*.

After climbing 34 percent in 2010, the number of federal and state wiretaps reported in 2011 decreased 14 percent. A total of 2,732 wiretaps were reported as authorized in 2011, with 792 authorized by federal judges and 1,940 authorized by state judges. Two federal wiretap applications reported this year for a previous reporting period were denied. Compared to the numbers approved during 2010, the number of applications reported as approved by federal judges declined 34 percent in 2011, and the number of applications approved by state judges fell 2 percent. The reduction in wiretaps resulted primarily from a drop in applications for narcotics offenses.

Wiretap applications in California, New York, and New Jersey accounted for 62 percent of all applications approved by state judges (see table below). In 2011, a total of 127 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, compared to 106 in 2010.

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 2011, the average length of an original authorization was 29 days, the same average length as in 2010. In total, 1,777 extensions were requested and authorized in 2011, a decrease of 8 percent. The average length of an extension was 29 days. For federal intercepts terminated in 2011, the longest intercept occurred in the Western District of Washington, where the original order was extended eight times to complete a 246-day wiretap used in a narcotics investigation. A report for another federal wiretap that was submitted in 2011 for a previous reporting period indicated that an order in the Western District of Texas was extended 300 days for a corruption investigation. The longest state wiretap, which was used in a gambling investigation conducted by Queens County, New York, was employed for a total of 846 days. The second-longest state wiretap, which also was performed in Queens County, New York, was used in a narcotics investigation for a total of 668 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 2011, a total of 98 percent (2,674 wiretaps) of all authorized wiretaps were designated as portable devices.

States With Largest Numbers of Applications Approved by State Judges

State	Number of Applications	Percent of Total
California	630	32
New York	441	23
New Jersey	140	7

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 2011, three federal wiretaps were designated as roving. Eight 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 "other major offenses." Table 3 indicates that 85 percent of all applications for intercepts (2,334 wiretaps) in 2011 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 Western District of Texas (94 applications), the Northern District of Illinois (61 applications), and the District of Arizona (54 applications). On the state level, the largest numbers of drug-related wiretaps were reported by Los Angeles County of California (161 applications), Riverside County of California (154 applications), and Queens County of New York (122 applications). Nationally, homicide was specified as the most serious offense in 4 percent of applications; "other major offenses" were 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 2011. Federal and state judges submitted 423 reports and 67 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, 2011. 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 2011, installed wiretaps were in operation for an average of 42 days, 2 days more than in 2010. The federal wiretap associated with the most intercepts occurred in the Eastern District of Michigan, where a narcotics investigation involving cellular telephones resulted in the interception of 71,195 messages over 202 days. The second-highest number of intercepts stemmed from a cellular telephone and other electronic device wiretap for a narcotics investigation in the Northern District of Indiana; this wiretap was active for 82 days and resulted in a total of 30,398 interceptions.

The state wiretap with the most intercepts was conducted by the New York Organized Crime Task Force, which performed a 564-day wiretap in a narcotics investigation involving cell phone interceptions that resulted in the interception of 274,219 messages. Another wiretap installed by the New York Organized Crime Task Force lasted 400 days and generated 135,072 cellular telephone and oral microphone 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 2011, encryption was reported during 12 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 2011. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 2,034 authorizations for which reports included cost data. The average cost of intercept devices in 2011 was $49,629, down 1 percent from the average cost in 2010. For federal wiretaps for which expenses were reported in 2011, the average cost was $71,748, a 13 percent increase from 2010. The cost of a state wiretap ranged from a low of $200 in Hudson County, New Jersey, to a high of $2,885,712 for a narcotics investigation conducted 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 96 percent (2,092 cases) of the intercepts installed in 2011, 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, 2011, a total of 3,547 persons had been arrested (down 25 percent from 2010), and 465 persons had been convicted (down 42 percent from 2010). Federal wiretaps were responsible for 28 percent of the arrests and 10 percent of the convictions arising from wiretaps for this period. The Eastern District of Missouri reported the most arrests for a wiretap in 2011—a wiretap used in a narcotics investigation in that district yielded the arrest of 64 individuals. A racketeering investigation in the Central District of California for 2007 resulted in the arrest of 93 individuals with 23 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. As part of a nationwide coordinated effort in a federal narcotics investigation, a wiretap in the District of Oregon uncovered incriminating cellular telephone communications and text messages that led to the arrest of 15 individuals and the seizure of luxury vehicles valued at nearly $600,000, about $250,000 in cash, and 14,000 oxycodone pills.

State Wiretaps Resulting in the Most Arrests

County and State	Type of Offense	Number of Arrests
Maricopa, AZ	Narcotics	111
Baltimore City, MD	Narcotics	65
Queens, NY	Narcotics	56

In the Eastern District of Michigan, the reporting officials stated that a narcotics investigation identified illegal activity that resulted in the arrests of 26 individuals and the seizure of $3,860,000 in cash, 12 vehicles, 3 firearms, and controlled substances. At the state level, a wiretap in a narcotics investigation in Maricopa County, Arizona, revealed several bank accounts used by a money-laundering organization and resulted in the seizure of $4,000,000. Several separate state jurisdictions reported that interceptions were instrumental in uncovering drug-trafficking organizations operating in the United States.

Summary of Reports for Years Ending December 31, 2001 Through 2011

Table 7 presents data on intercepts reported each year from 2001 to 2011. The number of authorized intercept applications reported by year increased 61 percent between 2001 and 2011 (the total for 2001 was revised after its initial publication). The majority of the wiretaps have consistently been used for drug crime investigations, which accounted for 78 percent of intercepts in 2001 (1,167 applications) and 85 percent in 2011 (2,334 applications). Table 9 presents the total numbers of arrests and convictions resulting from intercepts terminated in calendar years 2001 through 2011.

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 2011, a total of 4,006 arrests, 2,700 convictions, and additional costs of $51,874,823 arose from and were reported for wiretaps completed in previous years. Fifty-seven percent of the supplemental reports of additional activity in 2011 involved wiretaps terminated in 2010. Interceptions concluded in 2010 led to 61 percent of arrests, 45 percent of convictions, and 68 percent of expenditures noted in the supplementary reports.