

**CENTER FOR DEMOCRACY & TECHNOLOGY**[Our Mission](#) / [Get Involved](#) / [Staff](#) / [Publications](#) / [Links](#) / [Search CDT](#) / [Jobs](#) / [Action!](#)

October 3, 2001

**Government Surveillance**

## The Nature and Scope of Governmental Electronic Surveillance Activity

---

September 2001

As expanded wiretap authorities are proposed in response to the September 11, 2001 terrorist attacks, it is useful to first understand the current laws on electronic surveillance. Contrary to some of the assertions being made in support of new authorities, federal agencies already have broad legal powers to carry out wiretaps of telephone conversations, e-mail, pagers, wireless phones, computers and all other electronic communications and communications devices.

### -- Government wiretap authority

There are two sources of authority for wiretapping in the US.

(1) The Federal Wiretap Act, adopted in 1968 and sometimes referred to as Title III, normally requires, before a wiretap can commence, a court order issued by a judge who must conclude, based on an affidavit submitted by the government, that there is probable cause to believe that a crime has been, is being or is about to be committed. Terrorist bombings, hijackings and other violent activities are crimes for which wiretaps can be ordered. (Some relatively new criminal statutes on terrorism had not, as of Sept. 11, been added to the list of "predicate" crimes for which wiretaps could be ordered.) The government can and frequently does wiretap in advance of a crime being perpetrated. Judges almost never deny government requests for wiretap orders.

(2) The Foreign Intelligence Surveillance Act of 1978 allows wiretapping of aliens and citizens in the US based on a finding of probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power. For US citizens and permanent resident aliens, there must also be probable cause to believe that the person is engaged in activities that "may" involve a criminal violation. Suspicion of illegal activity is not required in the case of aliens who are not permanent residents.

Finally, it is worth noting that there are no legislative limits on US government electronic eavesdropping carried out overseas. Neither Title III nor FISA have any application to intelligence collection activities outside the US. The legal authority for electronic surveillance outside the US is contained in Executive Order 12333 issued by President Reagan in 1982, still in effect today. Intelligence agencies do not need a court order to intercept communications outside the US. If a United States citizen or US permanent resident alien is targeted for surveillance abroad, the Executive Order requires the approval of the Attorney General. By internal guideline, the Attorney General must find that there is probable cause to believe that the US person who is the target of the surveillance is an agent of a foreign power. Decisions to target non-US persons are left to the intelligence community. And the vacuum cleaner approach that does not involve targeting of US persons also requires no approval from outside the intelligence community, although there are limits on the dissemination of information about US persons that is collected "incidental" to an intelligence collection activity.

### -- Emergency authority

Both Title III and FISA allow the government to carry out wiretaps without a court order in emergency situations involving risk of death or serious bodily injury and in national security cases.

### -- Roving taps

Under Title III, the government has "roving tap" authority, meaning that it can get a court order that does not name a specific telephone line or email account but allows the government to tap any phone line, cell phone or Internet account that a suspect uses. This authority was initially adopted in 1986 and was substantially broadened in 1999.

Roving taps are relatively rare. In 2000, 27 roving taps were approved. Of those, seven were for federal investigations: three for use in drug offense investigations, one in a murder investigation, one in a gambling investigation, one in a racketeering investigation, and one in a firearms investigation. On the state level, 20 roving wiretaps were reported; 60 percent (12 applications) were authorized for use in drug offense investigations, 10 percent (2 applications) in bribery investigations, and the remainder (six applications) in investigations of other offenses. The 2000 Wiretap Report, issued in April 2001, is available online at <http://www.uscourts.gov/wiretap00/contents.html>

### -- Encryption

Beginning with the 2000 Wiretap Report, the government is required to report on 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 2000, no federal wiretaps reported that encryption was encountered. For state and local jurisdictions, encryption was reported to have been encountered in 22 wiretaps in 2000; however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted.

### -- Courts Rarely Deny Wiretap Requests

The rapid changes in telecommunications technology have been accompanied by a growth in the potential intrusiveness of electronic surveillance and a steady increase in government surveillance activity. While the wiretap laws establish important protections -- most notably requiring for interception of call content a judicial order based on a finding of probable cause -- in practice state and federal judges rarely deny applications for authority to conduct electronic surveillance.

Every spring, the Administrative Office of the United States Courts publishes statistics on wiretap activity of federal, state and local police in the prior year. The report covering 2000 is available online: <http://www.uscourts.gov/wiretap00/contents.html>. A useful summary, covering the years 1990-2000 and showing the nearly steady increase in the use of wiretaps, is provided by Table 7, which is at <http://www.uscourts.gov/wiretap00/table700.pdf>.

## -- Highlights of the 2000 Report on Wiretaps in Criminal Cases

Number of wiretap requests approved in 2000: **1,190**

Number of wiretap requests denied: **0**

Percent in which the most serious crime was a drug-related crime: **75%**

Percent in which encryption prevented law enforcement from receiving the plain text of intercepted communications: **0%**

Average number of conversations intercepted per wiretap: **1,769**

Average number of people intercepted per wiretap: **196**

Approximate number of conversations intercepted: **2.1 million**

Longest running wiretap: **308 days**

Percent of intercepted conversations deemed "incriminating": **23%**

Average cost of wiretap: **\$54,829**

## -- Recent Trends

Year	Applications	Wiretap orders approved
2000	1190	1190
1999	1350	1350
1998	1329	1327
1997	1186	1186
1996	1150	1149

Prior to 1996, the last time that any application, state or federal, for electronic surveillance was denied was 1988, when 2 out of 738 applications were denied. Meanwhile, from 1990 through 2000, 12,039 applications were approved. Wiretap authorizations have increased 55% since 1990, when there were 872.

These figures do not include consensual wiretaps, bugs and body wires, where a crime victim, an informant or an undercover agent consents to the recording of a conversation to which he or she is a party. Such interceptions, a staple of modern law enforcement practice, usually are not reflected in the statistics since, under federal law and the law of most states, they do not require court approval.

## Foreign Intelligence Surveillance

Nor does the figure of 1,190 approved wiretaps for 2000 cover the separate set of authorizations issued by a select group of federal judges, operating under the Foreign Intelligence Surveillance Act (FISA), who yearly issue over 1000 interception and secret physical search orders in foreign counterintelligence and international terrorism cases (1012 in 2000). (It is hard to tell, given the classified nature of the court's proceedings, how many wiretaps these orders entail. Some of the orders are good for one year, while some require reauthorization every ninety days, so some targets are the subject of four orders in a year. On the other hand, one order may authorize multiple taps. Plus, starting in 1996, the figures for the FISA court included physical searches ("black bag jobs") which are probably relatively few in number.) In its entire existence, since 1978, the FISA court has turned down only one government request for electronic surveillance authority.

## Real-time Collection of Call-Identifying Information

The figures on court ordered wiretaps (interceptions of the content of conversations) also do not include orders issued on a lower standard for surveillance of transactional data through pen registers and trap and trace devices. In 1996, law enforcement agencies in the U.S. Department of Justice alone obtained a total of 4569 original pen register or trap and trace orders, authorizing contemporaneous interception of dialed number information on the telephone facilities of 10,520 persons. This compares with 4972 orders in 1995, covering the telephone facilities of 11,801 persons. There are never any denials of pen register and trap and trace requests, since the law provides that the judge "shall" issue the order whenever an attorney for the government certifies that the information likely to be obtained is "relevant" to an ongoing criminal investigation. These statistics cover only the law enforcement agencies of the U.S. Department of Justice. They do not cover other federal law enforcement agencies or state and local police. (In 1994 Congressional testimony, the FBI Director estimated that the total number of pen register orders in 1992 was 9,000.)

## Subpoenas for Call-Identifying Information

Finally, a full picture of government surveillance activity must include cases in which law enforcement uses a subpoena to obtain stored transactional records relating to local or long distance calls. Companies collect and store such information for billing and other business purposes, and law enforcement agencies routinely request them in criminal cases, usually with a grand jury subpoena. (In foreign counterintelligence and international terrorism cases, the FBI can obtain such information without a court order.) Data on these cases are not assembled by the government. However, the scope of law enforcement activity is suggested by data submitted by some telephone service providers in response to a congressional inquiry in 1993. Bell Atlantic, for example, indicated that for the years 1989 through 1992, it had responded to 25,453 subpoenas or court orders for toll billing records of 213,821 of its customers. NYNEX reported that it had processed 25,510 subpoenas covering an unrecorded number of customers in 1992 alone.

## The Legal Protections and Their Erosion Over Time

The wiretap laws include several protections against abuse. Illegally seized evidence cannot be used in court. The exclusionary rule in the Fourth Amendment to the Constitution is bolstered by a statutory exclusionary rule in the federal wiretap statute, making evidence obtained from illegal wiretaps useless in court. (The Clinton Administration proposed weakening the statutory exclusionary rule, to make the introduction of illegal wiretap evidence easier.)

However, it must also be said that judges tend to give law enforcement agencies broad latitude, as reflected in judicial decisions approving law enforcement conduct when defendants seek to suppress wiretap evidence at trial. Between 1985 and 1994, judges nationwide granted 138 suppression motions while

denying 3060 for a 4.3% suppression rate.

One of the most significant areas in which the courts have expansively interpreted the law concerns the question of necessity. The wiretap law states that the court cannot approve an interception request unless it finds that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." Law enforcement officials regularly contend, as FBI Director Freeh did in 1994 testimony, that this provision of the law permits electronic surveillance "only when all other investigative techniques will not work or are too dangerous" (emphasis added). In practice, the courts have interpreted this provision to require only that law enforcement try some other techniques, not that they exhaust all reasonably available methods of obtaining the necessary evidence.

Courts have also been reluctant to enforce the minimization requirements of the law, which require law enforcement agents to screen the calls and turn off their recording devices whenever the conversation appears to relate to irrelevant, non-incriminating aspects of the target's life. Judges rarely rule that a wiretap was illegally carried out for failure to minimize.

September 2001

---

[ [Other CALEA Issues](#) ]

