Order Code 98-327
Updated September 2, 2008

CRS Report for Congress

Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

Gina Marie Stevens and Charles Doyle
American Law Division

Summary

It is a federal crime to intentionally wiretap or electronically eavesdrop on the conversation of another without a court order or the consent of one of the parties to the conversation. Moreover, in eleven states, it is a state crime for anyone other than the police to intentionally wiretap and/or electronically eavesdrop on the conversation of another without the consent of *all* of the parties to the conversation. The federal crimes are punishable by imprisonment for up to five years and expose offenders to civil liability for damages, attorneys' fees, and possibly punitive damages. State crimes carry similar consequences. Even in states where one party consent interceptions are legal, they may well be contrary to the professional obligations of members of the bar. The proscriptions often include a ban on using or disclosing the fruits of an illegal interception.

Statutory exceptions to these general prohibitions permit judicially supervised wiretapping or electronic eavesdropping conducted for law enforcement or foreign intelligence gathering purposes. Similar regimes — proscriptions with exceptions for government access under limited circumstances — exist for telephone records, e-mail and other forms of electronic communications.

The first federal wiretap statute was a World War I provision enacted for the duration of the conflict and designed to protect confidential government information (citation for the authority for this and other statements made throughout this report may be found in the long version of this report, CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*). The 1927 Radio Act outlawed intercepting and divulging private radio messages. The 1934 Communications Act extended the interception and divulgence ban to telephone and telegraph communications.

No federal law condemned secretly capturing face to face conversations by using hidden microphones or their ilk, and police and federal authorities employed them with increasing regularity. Then in the late 1960's, the Supreme Court held that the privacy

protection afforded by the Fourth Amendment's warrant requirements enveloped all that over which an individual might have a "justifiable expectation of privacy" — including, under the appropriate circumstances, the individual's conversations.

In anticipation of the Court's announcement, several states had enlarged the powers of their courts to issue wiretapping and/or electronic eavesdropping warrants. The Court, however, found one of the more detailed of these constitutionally deficient. Congress responded with Title III of the Omnibus Crime Control and Safe Streets Act to provide a constitutionally viable procedure under which state and federal courts might approve wiretapping and electronic eavesdropping orders. Title III at the same time outlawed wiretapping and electronic eavesdropping except under court order or with the consent of one of the parties to the conversation.

Title III regulated capture of the spoken word, it did nothing to protect the more modern forms of communication — fax messages, e-mail, electronically transmitted data. Congress recast Title III in the Electronic Communications Privacy Act (ECPA) to correct this oversight. It responded to a Supreme Court opinion again — this one describing the President's inherent authority to approve warrantless wiretapping of purely domestic threats to national security — with the Foreign Intelligence Surveillance Act (FISA). FISA creates a judicial warrant procedure for foreign intelligence information gathering.

Crimes

Title III/ECPA bars the use of any mechanism (device), tape recorder included, to intentionally capture the spoken word or any communication being transmitted electronically (intercept wire, oral, or electronic communications) without the consent of one of the participants or a court order, 18 U.S.C. 2511(1)(a),(b). This applies to all telephone conversations whether a cell telephone is involved or not. It likewise applies to all face to face conversations unless they occur in a public place or under other circumstances where the speakers should reasonably have expected that their conversation would be overheard.

Most states have similar statutes, and even when it is not a federal crime, wiretapping and/or electronic eavesdropping by anyone other than the police is a state crime (under mens rea requirements that vary from state to state) when done without the consent of *all* parties to the conversation in California, Delaware, Florida, Illinois, Kansas, Maryland, Massachusetts, Montana, Oregon, Pennsylvania, and Washington.

Beyond interception (wiretapping or electronic eavesdropping), it is a federal crime:

- to endeavor to illegally intercept;
- to procure another to illegally intercept;
- to disclose information gained from an illegal interception, knowing or having reason to know that the information is the product of an illicit interception;
- to endeavor to knowingly disclose illegally intercepted information;
- to procure another to disclose illegally intercepted information;
- to endeavor to disclose or to disclose information:
  - knowing it was gained from a court ordered interception,

  - having acquired the information during a criminal investigation, and
  - intending to improperly obstruct a criminal investigation by the disclosure;
- to access stored e-mail communications or telephone records unlawfully;
- to use a trap and trace device or a pen register (machines that record the origin of income or the destination of outgoing calls respectively) without court approval or individual consent; or
- to abuse eavesdropping authority under the Foreign Intelligence Surveillance Act.

Violators face imprisonment for up to five years, fines of up to $250,000 ($500,000 for organizations); and civil liability to actual or liquidated damages, attorneys' fees, possibly punitive damages, and administrative or professional discipline. The products of illegal interceptions are inadmissible as evidence in either federal or state proceedings.

Procedure

Senior Justice Department officials or chief state or local prosecutors may authorize an application for court ordered wiretapping or electronic eavesdropping as part of the investigation of a list of predicate crimes. Applications and court orders authorizing interception include specifics as to the individuals and the details of the crime, the communication facilities or place where the interception is to occur, the communications to be intercepted, the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted, why alternative investigative methods would be futile or dangerous, the duration of the proposed interception, steps taken to avoid interception of innocent communications, the history of any prior interceptions, the nature of third party assistance required and the identity of those to provide it, and any additional information the judge may require.

A court may issue an order upon a finding of probable cause with respect to the offense, the suspect, the conversation, and futility or dangers associated with alternative methods. The orders are good for a maximum of 30 days, with the possibility of 30 day extensions. Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order.

Within 90 days of the expiration of the termination of the order those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days advance notice to the parties. Information secured through a court ordered interception may be disclosed to law enforcement or intelligence officers for the performance of their official duties and as evidence during legal proceedings.

In emergency cases involving organized crime, threats to national security, or immediate danger of death or serious injury, interceptions may be authorized by senior officials before the issuance of an order. In such cases, court approval must be sought within 48 hours and the interception abandoned and an inventory of the results turned over to the communicants, if approval is denied.

Any federal prosecutor may approve an application for a court order authorizing the interception of e-mail or other electronic communications upon probable cause of a felony and the other requirements for issuance and execution of a search warrant. With regard to stored e-mail or voice mail, communications in remote storage, and telephone and service provider records, government officials may gain access to electronic communications in electronic storage for less than six months under a search warrant issued upon probable cause to belief a crime has been committed and the search will produce evidence of the offense.

The government must use the same procedure to acquire older communications or those stored in remote computer storage if access is to be afforded without notice to the subscriber or customer. If the government officials are willing to afford the subscriber or customer prior notice, access may be granted under a court order showing that the information sought is relevant and material to a criminal investigation or under an administrative subpoena, a grand jury subpoena, a trial subpoena, or court order. General identifying and billing information is available to the government pursuant to an administrative subpoena, a grand jury or trial subpoena, a warrant, with the consent of the subscriber or customer, or under a court order issued with a showing that information is relevant and material to a criminal investigation.

Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information to be produced is relevant to a pending criminal investigation.

The approval procedure under the Foreign Intelligence Surveillance Act (FISA) is the most distinctive of the wiretap-related procedures. First, its focus is different. It is designed to secure foreign intelligence information not evidence of a crime (although the prospect of securing evidence is not disqualifying as long as there is a measurable foreign intelligence purpose); it operates in a highly secretive manner; and it is conducted entirely before the judges of an independent court convened for no other purpose.

The contents of FISA surveillance application and subsequent order include the identity of the applicant and an authorizing official; particularized information concerning the facilities or locations involved in the interception and of the foreign agent or power whose communications are the target of the interception; a detailed description of the communications to be intercepted and a summary of the minimization procedures to be followed; certification that the information cannot reasonable be obtained using alternative means; whether the information relates to a foreign attack, sabotage, terrorism or foreign clandestine intelligence activities; the means of accomplishing the interception; a history of past related applications; the term of the interception; any other information the judge requests.

FISA court judges issue orders approving electronic surveillance upon a finding that the application requirements have been met and that there is probable cause to believe that the target of the interceptions is a foreign power or the agent of a foreign power and the targeted places or facilities are used by foreign powers of their agents. As in the case of law enforcement wiretapping and electronic eavesdropping, there is authority to intercept prior to approval in emergency situations, but there is also statutory authority for a foreign intelligence surveillance interception without a court order when the communications

sought are limited to those among or between foreign powers or involve nonverbal communications from places under the open and exclusive control of a foreign power. The second of these is replete with reporting requirements to Congress and the FISA court.

In addition to surveillance provisions, FISA authorizes court orders in foreign intelligence cases for physical searches, the use of pen registers and trap and trace devices, and for the release of business records and other tangible items. The physical search sections mirror those governing electronic surveillance. FISA pen register and trap and trace procedures are similar to those of their law enforcement counterparts in ECPA, but with many of the attributes of other FISA provisions. The orders may be issued either by a member of the FISA court or by a FISA magistrate upon the certification of a federal officer that the information sought is likely to be relevant to an investigation of international terrorism or clandestine intelligence activities. They allow the Attorney General to authorize emergency installation and use as long as the application for an authorizing court order is filed within 48 hours and restrict the use of any resulting evidence if an order is not subsequently granted. The provisions for use of the information acquired run parallel to those that apply to FISA surveillance and physical search orders.

The USA PATRIOT Act and later the USA PATRIOT Improvement and Reauthorization Act temporarily rewrote the FISA business records procedure that expires on December 31, 2009. In its temporary form FISA orders may apply to any tangible property relevant to foreign intelligence investigation. Recipients may challenge the legality of the order and ask that its secrecy requirements be lifted or modified. As additional safeguards, Congress insisted upon the promulgation of miminization standards; established use restrictions; required the approval of senior officials for orders covering library and certain other types of records; confirmed and reenforced reporting requirements; and directed the Justice Department's Inspector General to conduct an audit of the use of the FISA tangible item authority.

Protect America Act. The Protect America Act (P.L. 110-55), which has since expired, granted the Attorney General and the Director of National Intelligence the power, under limited conditions, to authorize gathering foreign intelligence information, including by electronic surveillance, (for up to a year) relating to persons believed to be overseas. In order to exercise that power, the Attorney General and the Director of National Intelligence were required to certify under oath that the collection effort involved: (1) procedures reasonably calculated to assure that the information sought concerned a person outside the United States; (2) communications to which service providers or others had access; (3) a desire, at least in significant part, to gather foreign intelligence information; (4) accompanying minimization procedures; and (5) no electronic surveillance other than that directed at a person reasonably believed to be abroad, 50 U.S.C. 1805b(a)(expired).

That having been done or in emergency situations with their oral approval, the Attorney General and Director of National Intelligence might direct the communications providers, or others with access, to immediately assist in the gathering of the foreign intelligence information in a manner least disruptive of service to the target and under confidentiality restrictions imposed by the Attorney General and the Director of National Intelligence. The directive came with the promise of compensation at prevailing rates as

well as immunity from civil liability and was enforceable through the contempt power of the FISA court. Recipients were entitled to seek judicial modification of a directive, issued contrary to the statute or otherwise unlawfully, in the FISA court under expedited procedures.

The FISA court was also tasked with the responsibility of reviewing the procedures crafted to ensure that the authority was only invoked with respect to persons reasonably believed to be found overseas. Should the court have determined that the procedures were clearly erroneous, the government was free to amend them or to appeal the determination initially to the Foreign Intelligence Surveillance Court of Review and then to the Supreme Court.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (P.L. 110-261). P.L. 110-261 (H.R. 6304), signed July 10, 2008, addresses four FISA-related matters. First, in a manner reminiscent of the Protect America Act, it provides temporary authority to gather foreign intelligence information from or relating to overseas targets. Second, it reasserts the exclusivity of FISA and Title III/ECPA as a basis for governmental electronic surveillance. Third, it instructs the Inspectors General in various agencies to conduct a review and report to Congress on the Terrorist Surveillance Program. Fourth, it seeks to protect those who assist government surveillance activities from civil liability.