Order Code 98-327
Updated August 8, 2001

CRS Report for Congress

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

Gina Stevens
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 5 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. The First Amendment, however, precludes punishing anyone who acquires the information innocently from disclosing the results of an illicit interception dealing with matters of great public concern.

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 House Crime Subcommittee has held hearings on H.R. 1877, the Child Sex Crimes Wiretapping Act of 2001, which would permit court supervised wiretaps in certain child sex crime investigations. Similar proposals have been offered in the Senate and identical legislation passed the House at the close of the last Congress.

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 entitled, *Privacy: An Overview of Federal Statutes*

Governing Wiretapping and Electronic Eavesdropping, CRS Report 98-326 (2001)). 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 respond 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.

In a more recent adjustment, the Communications Assistance for Law Enforcement Act (CALEA) established a procedure designed to help police keep pace with advancing telecommunications advances and to provide tighter protection for e-mail and cordless telephone communications.

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.

With the exception of offenders who intentionally intercept certain cellular phone conversations, public CB communications, or pager messages (all less severely punished), violators face imprisonment for up to 5 years, fines of up to $250,000 ($500,000 for organizations); and civil liability to actual or liquidated damages, attorneys' fees, and possibly punitive damages. The products of illegal interceptions are inadmissible as evidence in either federal or state proceedings.

Following the lead of the American Bar Association, a majority of the states require that members of the legal profession refrain from secretly recording telephone or face to face conversations except in the performance of law enforcement duties, even in those jurisdictions where one party consent interceptions are not unlawful. A few jurisdictions have taken a contrary position or granted broader exceptions.

The Supreme Court recently clarified the extent to which the First Amendment right of free speech precludes a ban on disclosing the fruits of an illegal interception. The Amendment protects anyone who, having played no role in an illegal interception of communications dealing with matters of great public concern, discloses information from the pilfered conversation, *Bartnicki v. Vopper*, 121 S.Ct. 1753 (2001).

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 and 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 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 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, communications in remote storage, and telephone and service provider records, government officials may gain access to electronic communications in electronic storage for less than 6 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 afford 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; 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 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 (not longer than 90 days with extension possible for up to 1 year); 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.

Once Nettlesome Problems

Three issues related to wiretapping and electronic eavesdropping once proved especially challenging: encryption, telephony, and cell phone protection.

Encryption is the scrambling of the computer generated or computer stored communications. It can help ensure individual privacy and valuable security for trade secrets and confidential government information. It can also frustrate law enforcement and intelligence gathering activities. Proposals have been offered to guarantee a system under which the government would have real time, confidential access to the keys to lock any encrypted information when the circumstances warranted. Government procurement and export limitations have been used to encourage movement towards that goal. There have been objections.

Congress was uneasy over the application of wiretapping and eavesdropping prohibitions to those cell phone conversations that under an earlier technology were suspectable to inadvertent interception. Thus, while banning the intentional interception of cell phone conversations, Congress established a reduced penalty scheme for such interceptions under some circumstances for first time offenders acting without criminal, tortious or commercial motivation.

The companies that provide telephone and other communications service have long cooperated in law enforcement execution of court order wiretaps and electronic eavesdropping. Digital telephony and the explosion of other technological advances have made that assistance both more difficult and more expensive. Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to help pay communication service providers for the cost of configuring their systems to accommodate law enforcement needs. Initially, intervening technological developments and changing patterns of use complicated implementation efforts.

Legislation

H.R. 1877, the Child Sex Crimes Wiretapping Act of 2001, introduced by Representative Johnson, has been the subject of hearings before the House Crime Subcommittee, *hearing statements at, www.house.gov/judiciary/crime*. The bill, as introduced, is comparable to proposals offered in the Senate during this Congress (S. 1232 (Sen. McConnell) and S. 1234 (Sen. Hatch)) and virtually identical to legislation (H.R. 3484) passed by the House under suspension of the rules at the close of the 106th, 146 *Cong.Rec.* H8697-699 (daily ed. Oct. 3, 2000); *see also*, H.Rept. 106-920 (2000). It would authorize law enforcement officials to intercept Internet and other wire, oral and electronic communications under court order when conducting investigations of child pornography (18 U.S.C.2252A) or certain child sex abuse offenses (violations of 18 U.S.C. 2422 (coercion and enticement to travel interstate for sexual purposes) and 2423 (interstate transportation of minors for sexual purposes) which would be contrary to 18 U.S.C. ch.109A (sexual abuse of children) or ch.110 (sexual exploitation of children) if committed within a federal enclave).