102nd Congress
2nd Session

S. _____
[H.R. _____]

IN THE SENATE
[IN THE HOUSE OF REPRESENTATIVES]

M. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To ensure the continuing access of law enforcement to the content of wire and electronic communications when authorized by law and for other purposes.

Be it enacted by the Senate and the House of Representatives of the United States of America in Congress assembled,

SEC. 1. FINDINGS AND PURPOSES.

(a) The Congress finds:

(1) that telecommunications systems and networks are often used in the furtherance of criminal activities including organized crime, racketeering, extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs;

(2) that recent and continuing advances in telecommunications technology, and the introduction of new technologies and transmission modes by the telecommunications industry, have made it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept wire and electronic communications and thus threaten the ability of such agencies effectively to enforce the laws and protect the national security; and

(3) that without the assistance and cooperation of providers of electronic communication services and private branch exchange operators, the introduction of new technologies and transmission modes into telecommunications systems without consideration and accommodation of the need of government agencies lawfully to intercept wire and electronic communications would impede the ability of such agencies effectively to carry out their responsibilities.

(b) The purposes of this Act are to clarify the responsibilities of providers of electronic communication services and private branch exchange operators to provide such assistance as necessary to ensure the ability of government agencies to implement lawful court orders or authorizations to intercept wire and electronic communications.

SEC. 2. (a) Providers of electronic communication services and private branch exchange operators shall provide within the United States capability and capacity for the government to intercept wire and electronic communications when authorized by law:

(1) concurrent with the transmission of the communication to the recipient of the communication;

(2) in the signal form representing the content of the communication between the subject of the intercept and any individual with whom the subject is communicating, exclusive of any other signal representing the content of the communication between any other subscribers or users of the electronic communication services provider or private branch exchange operator, and including information on the individual calls (including origin, destination and other call set-up information), and services, systems, and features used by the subject of the interception;

(3) notwithstanding the mobility of the subject of the intercept or the use by the subject of the intercept of any features of the telecommunication system, including, but not limited to, speed-dialing or call forwarding features;

(4) at a government monitoring facility remote from the target facility and remote from the system of the electronic communication services provider or private branch exchange operator;

(5) without detection by the subject of the intercept or any subscriber; and

(6) without degradation of any subscriber's telecommunications service.

(b) Providers of electronic communication services within the public switched network, including local exchange carriers, cellular service providers, and interexchange carriers, shall comply with subsection (a) of this section within eighteen months from the date of enactment of this subsection.

(c) Providers of electronic communication services outside of the public switched network, including private branch exchange operators, shall comply with subsection (a) of this section within three years from the date of enactment of the subsection.

(d) The Attorney General, after consultation with the Department of Commerce, the Small Business Administration and Federal Communications Commission, as appropriate, may except from the application of subsections (a), (b) and (c) of this section classes and types of providers of electronic communication services and private branch exchange operators. The Attorney General may waive the application of subsections (a), (b) and (c) of this section at the request of any

provider of electronic communication services or private branch exchange operator.

(e) The Attorney General shall have exclusive authority to enforce the provisions of subsections (a), (b) and (c) of this section. The Attorney General may apply to the appropriate United States District Court for an order restraining or enjoining any violation of subsection (a), (b) or (c) of this section. The District Court shall have jurisdiction to restrain and enjoin violations of subsections (a) of this section.

(f) Any person who willfully violates any provision of subsection (a) of this section shall be subject to a civil penalty of $10,000 per day for each day in violation. The Attorney General may file a civil action in the appropriate United States District Court to collect, and the United States District Courts shall have jurisdiction to impose, such fines.

(g) Definitions--As used in subsections (a) through (f) of this section--

(1) 'provider of electronic communication service' or 'private branch exchange operator' means any service or operator which provides to users thereof the ability to send or receive wire or electronic communication, as those terms are defined in subsections 2510(1) and 2510(12) of Title 18, United States code, respectively, but does not include the government of the United States or any agency thereof;

(2) 'communication' means any wire or electronic communication, as defined in subsections 2510(1) and 2510(12), of Title 18, United States Code;

(3) ‘intercept‘ shall have the same meaning as set forth in section 2510(4) of Title 18, United States Code; and

(4) ‘government' means the Government of the United States and any agency or instrumentality thereof, any state or political subdivision thereof, the District of Columbia, and any commonwealth, territory or possession of the United States.

DIGITAL TELEPHONY AND INTERCEPTION

BY

CRIMINAL LAW ENFORCEMENT AGENCIES

The telecommunications systems and networks are often used to further criminal activities including white collar and organized crime, racketeering, extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs. Accordingly, for many years, one of the most important tools in the investigation of crime for Federal and State criminal law enforcement agencies has been the court authorized interception of communications. As illustrated below, the majority of original authorizations to intercept wire or electronic communications are conducted by State criminal law enforcement agencies.

Interception Applications Authorized

	State	Federal	Total
1984	512	289	801
1985	541	243	784
1986	504	250	754
1987	437	236	673
1988	445	293	738
1989	453	310	763
1990	548	324	872
Total	3,440	1,945	5,385

Approximately, 3/8 of authorized interceptions were conducted by Federal agencies, while 5/8 of the authorized interceptions were conducted by State criminal law enforcement agencies.[11]

The recent and continuing advances in telecommunications technology, and the introduction of new technologies by the telecommunications industry, have made it increasingly difficult for

[11]Interceptions for foreign intelligence and counterintelligence purposes are not counted within the figures used here, but would likewise benefit from enactment of the legislation.

government agencies to implement lawful orders or authorizations to intercept wire and electronic communications, as well as to implement pen register and trap-and-trace court orders or authorizations. These new technologies inadvertently undermine the ability of criminal law enforcement agencies to enforce effectively the criminal laws and protect the national security. Without the assistance and cooperation of the telecommunications industry, these new technologies will impede the ability of the telecommunications industry, these new technologies will impede the ability of the government to enforce the criminal law. Accordingly, the purpose of this bill is to clarify the existing responsibilities of electronic communication services providers and private branch exchange operators, as established, for example, in 18 U.S.C. ____ 2518(4), 3124(A), (B), to provide such assistance as necessary to ensure the ability of government agencies to implement lawful orders or authorizations to intercept communications.

Over the past twenty-five years, the working relationship between the criminal law enforcement community, particularly the Federal Bureau of Investigation as the federal government's primary criminal law enforcement agency, and the telecommunications industry, in response to the appropriate court orders or authorizations, has provided government agencies with timely access to the signals containing the content of communications covered by the court orders or authorizations. As a general proposition, this has involved providing the means to acquire the communication as it occurs between two individual telephone users at a remote location, not dissimilar to a call in which the two originating parties do not know that a third party is listening, and in which the third party (the criminal law enforcement agency) records the authorized and relevant calls.

Historically, and with relatively few exceptions, the telecommunications industry has provided the criminal law enforcement community with the ability to monitor and record calls:

1. at the same time as the call is transmitted to the recipient;

2. in the same form as the content of the call was transmitted through the network, notwithstanding the use by the target of custom features of the network;

3. whether stationary or mobile;

4. at the government monitoring facility;

5. without detection by the target or others subscribers; and without degrading any subscriber's service.

However, the introduction of new technology has begun to erode the ability of the government to fully effectuate interceptions, pen registers and trap-and-race court orders or authorizations that are critical to detecting and prosecuting criminals. As technology has developed, the telecommunications industry has not always ensured the continued ability to provide the same services to the criminal law enforcement community. The telecommunications industry's introduction

of certain types of new technology poses real problems for effective criminal law enforcement. Legislation is necessary to ensure that the government will be provided with this capability and capacity in the future by all providers and operators and to maintain a level playing field among competitive providers and operators in the telecommunications industry.

There have been instances in which court orders authorizing the interception of communications have not been fulfilled because of technical limitations within particular telecommunications networks. For example, as early as 1986, limited capabilities became apparent in at least one network which will only be corrected later in 1992. This technical deficiency in a new technology forced criminal law enforcement agencies to prioritize certain interceptions to the exclusion of other court orders. Accordingly, for approximately six years, there have been court orders that have not been sought by the criminal law enforcement community or executed by the telecommunications industry and, as a consequence, important criminal investigations have not been brought to fruition or have been less than efficiently concluded. This is one classic example of new technology affecting adversely the criminal law enforcement community: a microcosm of what may be expected on a nationwide basis without enactment of this legislation.

Section 1 of the bill states Congressional findings and purpose.

Section 2 is divided into seven subsections. Subsection (a) establishes as a matter of law the responsibility of electronic communication services providers and private branch exchange operators to continue to provide, within the United States, the capability and capacity for criminal law enforcement agencies to intercept wire and electronic communications when authorized by law. These subsections delineate the existing attributes of wire or electronic communication interception.

1. Concurrent with Transmission. The application for a court order to intercept telecommunications conversations or data transmissions is rarely a leisurely process. For example, on the Federal side, the development of the required affidavits, submission to the Criminal Division of the Department of Justice for approval, transmission of approval to the Assistant United States Attorney, the appearance of the Assistant before a judge to request the order and the delivery of the judge's order to the appropriate telecommunications company is frequently completed in a very short time. However, crime waits for no one and the system for approval of interceptions must and does conform with the realities of the activity that is sought to be investigated and, if appropriate, prosecuted as criminal offenses. Since time is of the essence, current law requires that service providers and operators provide the government forthwith all information, facilities and technical assistance necessary to accomplish its mission. It is critical that the telecommunications industry respond quickly to execute the court order or authorization. The ultimate problem of timeliness, however, is the real-time monitoring of the intercepted communications. As serious and potentially life-threatening criminal conduct is detected, it may be necessary to move quickly to protect innocent victims from that conduct. Accordingly, "real-time" monitoring is critical.

2. Isolated Signal and Services Used. Nearly all of the communications network is partially "analog" at this time. In conducting an interception, for example, of a telephone conversation, the government is allowed to monitor and record criminal conversation such as a conspiracy, minimizing the acquisition of non-criminal or innocent conversation. When an electronic communication services provider or private branch exchange operator introduces a new technology--such as a digital signal--the communications are converted into a different and more efficient form for transmission, but a more difficult form to monitor during interception. The bill requires only that the provider or operator isolate and provide access to the electronic signal that represents the content of the communications of the target of the intercept[22] from the stream of electronic signals representing other communications. This provision seeks to ensure that, in the new electronic environment in which signals are mixed for transmission and separated at another switch for distribution, the government does not receive the communications of any individual other than the individuals using the target's communications point of origin and receipt; the government must remain subject to the minimization standards of 18 U.S.C. __ 2518(5).

This provision also makes it clear that an electronic communication services provider or private branch exchange operator is not required to provide for reconversion of the isolated communication to analog or other form. The government expects that this process will be accomplished by the government.

3. Mobility and Features. Increasingly, criminal acts are being conducted or discussed over cellular telephones or by using special telecommunications features. As this mobility is introduced, the electronic communication services providers and private branch exchange operators would be required to assure the capability and capacity for criminal law enforcement agencies to continue lawful interception.

Further, this subsection makes it clear that features used by the target do not defeat the court order or authorization. For example, communications which have been addressed to the telephone number of the target, but which may have been programmed through a call-forwarding feature to another, otherwise innocent, telephone number, must be captured and made available to criminal law enforcement authorities pursuant to court order or authorization. This requirement will obviate the need for applications for authority to monitor otherwise innocent telephone numbers that receive, only intermittently, calls forwarded by the target. The effect of this provision is to further minimize monitoring of calls of innocent parties. Similarly, certain speed dialing features that mask the telephone number called by the target must be identified for criminal law enforcement investigation. The ability to consistently determine the destination of calls is critical to minimizing the monitoring of innocent calls.

4. Government Monitoring Facility. Government agencies do not normally request the use of telecommunications industry physical

[22] Whether the content is voice, facsimile, imagery (e.g. video), computer data, signalling information, or other forms of communication, does not matter; all forms of communication are intercepted.

facilities to conduct authorized interceptions nor is it encourage by the industry. Normally, the government leases a line from the electronic communication services provider's or private branch exchange operator's switch to another location owned or operated by the government. This minimizes the cost and intrusiveness of interceptions, which benefits the service provider or operator, as well as the government. Accordingly, the ability to monitor intercepted communications remotely is critical.

5. Without Detection. One of the reasons that governments operate their own facilities is to reduce the risk of detection of the interception, which would render the interception worthless. At the present time, the existence of an interception is unknown to any subscriber and is not detectable by the target, notwithstanding folklore and spy novels. This provision merely ensures that the secrecy of effective interceptions will be maintained.

6. Without Degradation. Maintaining the quality of the telephone network is in the interest of the government, the industry and the public. Presently, the existence of an interception has no effect on the quality of the service provided by any network to the target or any subscriber. This provision ensures that the quality of the network will continue to be uncompromised. Absent the assistance delineated by this legislation, the execution of court orders and authorizations by the government could well disrupt service of the newer technological systems, a result that this legislation seeks to avoid.

Subsection (b) provides that electronic communication services providers and private branch exchange operators with the "public switched network" must be in compliance with the minimum intercept attributes within eighteen months after enactment. Thereafter, new technologies must continue to meet these minimum attributes.

Subsection (c) provides that electronic communication service providers and private branch exchange operators that are not within the "public switched network" must be in compliance with the minimum intercept attributes within eighteen months after enactment. Thereafter, new technologies must continue to meet these minimum attributes.

Subsection (d) provides that the Attorney General may grant exceptions to the affirmative requirements of subsection (a), as well as the implementation deadlines of subsections (b) and (c). In considering any request for exception, the Attorney General will consult with Federal Communications Commission, the Small Business Administration and the Department of Commerce, as appropriate. Accordingly, the Attorney General has the authority to except, for example, whole classes, categories or types of private branch exchange operators where no serious criminal law enforcement problems are likely to arise, such as hospital telephone systems.

This subsection also permits the Attorney General to waive the requirements of subsections (a), (b) and (c) on application by an electronic communication services provider or private branch exchange operator. Accordingly, if a particular company can not comply with one or more of the requirements of subsection (a), or needs time additional to that permitted under subsections (b) or (c), the Attorney General may grant an appropriate waiver.

Subsection (e) provides that the Attorney General has exclusive authority to enforce the provisions of the bill. While a number of States have authority to seek and execute interception orders, they will be required to seek the assistance of the Attorney General if enforcement of this legislation is required. This section also provides for injunctive relief from violations of the provisions of the bill.

Subsection (f) provides for enforcement of the provisions of the bill through imposition of civil fines against any company that is not excepted from the provisions of the bill, does not acquire a waiver of the provisions of the bill, and fails to meet the requirements of subsection (a) after the effective dates set out in subsection (b) or (c), as appropriate. A fine of up to $10,000 per day for each day in violation may be levied; for most companies in the telecommunications industry this amount is sufficient to ensure that compliance will be forthcoming. Although this provision is not expected to be used, it is critical to ensure that compliance with the provisions of the bill will occur after the effective dates of the requirements of subsection (a).

Subsection (g) carries forward a number of definitions from the current provisions for the interception of wire or electronic communications under "Title III." The definition of "government" that is currently in use includes all States, territories and possessions of the United States, as well as the United States, is made applicable to the bill.