Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. letter	Webster Hubbell to Leon Panetta re: Digital Telephony Legislation (3 pages)	02/18/1994	P1/b(1)

COLLECTION:

Clinton Presidential Records
Staff Secretary
John Podesta (Subject Files)
OA/Box Number: 17335

FOLDER TITLE:

Digital Telephony [1]

2018-0662-S
rs3150

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

John Tim

~~Floor debate~~

Pull

for H.R. 4922.

Senate

statements

on

~~Senate~~

— bill's passage

file digital telephony

bankruptcy professionals have expressed concern regarding the scope of section 312, it is my understanding that because of existing case law precedent relative to mail fraud, section 312 would only apply in cases where there existed proof beyond a reasonable doubt of a specific intent to defraud. In this regard, I attach an excerpt from a memorandum prepared by the Department of Justice acknowledging the very heavy burden they would face in bringing a fraud action under section 312.

INTENT TO DEFRAUD MUST BE PROVED BEYOND A REASONABLE DOUBT

Proposed §157(a), patterned after the mail and wire fraud statutes (18 U.S.C. §1341, 1343), would require proof of devising or intending to devise a "scheme or artifice to defraud." Like the mail fraud statute, an essential element of the proposed statute requires *proof beyond a reasonable doubt of a specific intent to defraud*. This is one of the highest *mens rea* standards in the criminal law. Because of this high burden of proof, courses of action permitted under the Bankruptcy Code and allowed by the bankruptcy courts are unlikely to be prosecutable under this new law or any fraud statute. Where a statute or case supports the action taken and the person can show that he or she relied on such law, it would not be possible to show the intent to defraud required by the statute proposed.

Knowledge and intent are elements in any fraud prosecution. *See, e.g., U.S.* v. *White*, 879 F.2d 1509, *cert. den.*, 494 U.S. 1027 (1990) (wife who had no knowledge of concealed business property could not be prosecuted for signing false statements that omitted such property); *U.S.* v. *Tashjian*, 660 F.2d 829, *cert. den.*, 454 U.S. 1102 (1982); *U.S.* v. *Martin*, 408 F.2d 949, *cert. den.*, 396 U.S. 824 (1970); *U.S.* v. *Goodstein*, 883 F.2d 1362 (7th Cir.), *cert. den.*, 494 U.S. 1007 (1990). Similarly, the requirement that any fraud be "material" (while not in any statutory language, "materiality" is an element of bankruptcy fraud as well) would contemplate and include a concept that the fraud would target and interfere with the bankruptcy process.

Because of this high burden of proof, most courses of action allowed by the bankruptcy courts are unlikely to be prosecutable under this new law or any fraud statute. Where a statute or case supports the action taken and the person can show that he or she relied on such law, it would be extremely difficult to show an intent to defraud. Good faith has long been recognized as a complete defense to any fraud prosecution. *See e.g., United States* v. *Williams*, 728 F.2d 1402 (11th Cir. 1984) (good faith is a complete defense to the element of intent to defraud). Advice of counsel is also a defense that will counter a fraud prosecution where a debtor took certain action based on an attorney's good faith interpretation of the bankruptcy laws.

The proposed statute is no broader than the mail fraud statute, and in many respects is narrower because of the body of bankruptcy law potential defendants could point to in justifying their actions. The courts have the ability to ensure that this proposed law is not abused, just as they have monitored the application of the criminal laws in other areas. For example, in prosecutions under the income tax laws, the courts have allowed good faith but mistaken and misguided reliance on civil laws to be raised as a defense to a criminal prosecution. *See e.g., United States* v. *Cheek*, —— U.S. ——, 111 S. Ct. 604 (1991).

Ms. SLAUGHTER. Mr. Speaker, I rise in strong support of H.R. 5116, the Bankruptcy Reform Act of 1994.

H.R. 5116 contains a number of improvements to the Bankruptcy Code, including expedited court procedure, increased protection against bankruptcy fraud, and the establishment of a National Bankruptcy Commission to pay close attention to key issues in bankruptcy procedure.

One section of H.R. 5116 which I feel is vitally important is similar to the text of my own bill, H.R. 4711, the Spousal Equity in Bankruptcy Amendments. Here, H.R. 5116 gives added protection to child support and alimony payments in the event of a bankruptcy filing. Under the current Bankruptcy Code, child support and alimony are given no priority when a debtor's assets are distributed. It is incomprehensible that while many creditors can collect their fees, dependent spouses and children have to wait, and may never be included. H.R. 5116 elevates child support from its current status as a general, unsecured debt to a formally prioritized debt. This import change will help ensure that a custodial parent will not have to wait years to receive payment due.

H.R. 5116 also closes a loophole which can be devastating for single-parent families. During a divorce agreement, it is not uncommon for the custodial parent to accept a lower level of child support in exchange for the other parent assuming the couple's marital debts. If the non-custodial parent declares bankruptcy, however, the marital debts than fall to the single parent. Think of what the custodial parent then faces: little or no child support payments, the heavy responsibilities of all the marital debts, and the expenses that come with rearing children alone.

The Bankruptcy Reform Act would obligate the non-custodial spouse, who agreed to pay the couple's marital debts, to continue responsibility for these debts. I think it is outrageous that wives and dependent children must answer to creditors for debts the husband first agreed to pay. This relatively small—but vital—change in the Bankruptcy Code would prevent this situation, and ensure a more equitable treatment of all parties in the event of bankruptcy.

Mr. Speaker, I have heard heartbreaking stories from single parents who want nothing but the best for their children, but find themselves forced to fight for their rightful level of child support. With no other recourse, these families often turn to welfare to provide the child support the absent parent ought to be responsible for. H.R. 5116 takes an important first step in breaking this tragic cycle by strengthening current bankruptcy law and enforcing tougher measures for child support and alimony collection.

Finally, Mr. Speaker, I would like to commend the distinguished Chairman of the Judiciary Committee, JACK BROOKS, and ranking member HAMILTON FISH, for their diligent efforts and hard work in moving omnibus bankruptcy reform before Congressional adjournment. I encourage my colleagues to join me in supporting the Bankruptcy Reform Act. Thank you, Mr. Speaker, and I yield back the balance of my time.

□ 2030

Mr. BROOKS. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. POSHARD). The question is on the motion offered by the gentleman from Texas [Mr. BROOKS] that the House suspend the rules and pass the bill, H.R. 5116, as amended.

The question was taken.

Mr. GEKAS. Mr. Speaker, I object to the vote on the grounds that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 5, rule I, and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

HOUR OF MEETING ON TOMORROW

Mr. FRANK of Massachusetts. Mr. Speaker, I ask unanimous consent that when the House adjourns today it adjourn to meet at 9:30 a.m. on tomorrow.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Massachusetts?

There was no objection.

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT AND SUNDRY AMENDMENTS TO THE CODE AND THE COMMUNICATIONS ACT OF 1934

Mr. BROOKS. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4922) to amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, as amended.

The Clerk read as follows:

H.R. 4922

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

TITLE I—INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

SEC. 101. SHORT TITLE.

This title may be cited as the "Communications Assistance for Law Enforcement Act".

SEC. 102. DEFINITIONS.

For purposes of this title—

(1) The terms defined in section 2510 of title 18, United States Code, have, respectively, the meanings stated in that section.

(2) The term "call-identifying information" means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

(3) The term "Commission" means the Federal Communications Commission.

(4) The term "electronic messaging services" means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.

(5) The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof author-

ized by law to conduct electronic surveillance.

(6) The term "information services"—

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes—

(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;

(ii) electronic publishing; and

(iii) electronic messaging services; but

(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

(7) The term "telecommunications support services" means a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network.

(8) The term "telecommunications carrier"—

(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

(B) includes—

(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))); or

(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title; but

(C) does not include—

(i) persons or entities insofar as they are engaged in providing information services; and

(ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.

SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS.

(a) CAPABILITY REQUIREMENTS.—Except as provided in subsections (b), (c), and (d) of this section and sections 108(a) and 109(b) and (d), a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier—

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains,

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects—

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

(b) LIMITATIONS.—

(1) DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS.—This title does not authorize any law enforcement agency or officer—

(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or

(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

(2) INFORMATION SERVICES; PRIVATE NETWORKS AND INTERCONNECTION SERVICES AND FACILITIES.—The requirements of subsection (a) do not apply to—

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

(3) ENCRYPTION.—A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

(c) EMERGENCY OR EXIGENT CIRCUMSTANCES.—In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of title 18, United States Code, and section 1805(e) of title 50 of such Code), a carrier at its discretion may comply with subsection (a)(3) by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

(d) MOBILE SERVICE ASSISTANCE REQUIREMENTS.—A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of wire or electronic communication service that has acquired access to the communications.

SEC. 104. NOTICES OF CAPACITY REQUIREMENTS.

(a) NOTICES OF MAXIMUM AND ACTUAL CAPACITY REQUIREMENTS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this title, after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, and after notice and comment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications industry associations and standard-setting organizations—

(A) notice of the actual number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph (B), that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously by the date that is 4 years after the date of enactment of this title; and

(B) notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this title.

(2) BASIS OF NOTICES.—The notices issued under paragraph (1)—

(A) may be based upon the type of equipment, type of service, number of subscribers, type or size or carrier, nature of service area, or any other measure; and

(B) shall identify, to the maximum extent practicable, the capacity required at specific geographic locations.

(b) COMPLIANCE WITH CAPACITY NOTICES.—

(1) INITIAL CAPACITY.—Within 3 years after the publication by the Attorney General of a notice of capacity requirements or within 4 years after the date of enactment of this title, whichever is longer, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of—

(A) accommodating simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under subsection (a)(1)(A); and

(B) expanding to the maximum capacity set forth in the notice under subsection (a)(1)(B).

(2) EXPANSION TO MAXIMUM CAPACITY.—After the date described in paragraph (1), a telecommunications carrier shall, subject to subsection (e), ensure that it can accommodate expeditiously any increase in the actual number of communication interceptions, pen registers, and trap and trace devices that authorized agencies may seek to conduct and use, up to the maximum capacity requirement set forth in the notice under subsection (a)(1)(B).

(c) NOTICES OF INCREASED MAXIMUM CAPACITY REQUIREMENTS.—

(1) NOTICE.—The Attorney General shall periodically publish in the Federal Register, after notice and comment, notice of any necessary increases in the maximum capacity

requirement set forth in the notice under subsection (a)(1)(B).

(2) COMPLIANCE.—Within 3 years after notice of increased maximum capacity requirements is published under paragraph (1), or within such longer time period as the Attorney General may specify, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of expanding to the increased maximum capacity set forth in the notice.

(d) CARRIER STATEMENT.—Within 180 days after the publication by the Attorney General of a notice of capacity requirements pursuant to subsection (a) or (c), a telecommunications carrier shall submit to the Attorney General a statement identifying any of its systems or services that do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under such subsection.

(e) REIMBURSEMENT REQUIRED FOR COMPLIANCE.—The Attorney General shall review the statements submitted under subsection (d) and may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for costs directly associated with modifications to attain such capacity requirement that are determined to be reasonable in accordance with section 109(e). Until the Attorney General agrees to reimburse such carrier for such modification, such carrier shall be considered to be in compliance with the capacity notices under subsection (a) or (c).

SEC. 105. SYSTEMS SECURITY AND INTEGRITY.

A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.

SEC. 106. COOPERATION OF EQUIPMENT MANUFACTURERS AND PROVIDERS OF TELECOMMUNICATIONS SUPPORT SERVICES.

(a) CONSULTATION.—A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching equipment and its providers of telecommunications support services for the purpose of ensuring that current and planned equipment, facilities, and services comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.

(b) COOPERATION.—Subject to sections 104(e), 108(a), and 109(b) and (d), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.

SEC. 107. TECHNICAL REQUIREMENTS AND STANDARDS; EXTENSION OF COMPLIANCE DATE.

(a) SAFE HARBOR.—

(1) CONSULTATION.—To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions.

(2) COMPLIANCE UNDER ACCEPTED STANDARDS.—A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

(3) ABSENCE OF STANDARDS.—The absence of technical requirements or standards for implementing the assistance capability requirements of section 103 shall not—

(A) preclude a telecommunications carrier, manufacturer, or telecommunications support services provider from deploying a technology or service; or

(B) relieve a carrier, manufacturer, or telecommunications support services provider of the obligations imposed by section 103 or 106, as applicable.

(b) COMMISSION AUTHORITY.—If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that—

(1) meet the assistance capability requirements of section 103 by cost-effective methods;

(2) protect the privacy and security of communications not authorized to be intercepted;

(3) minimize the cost of such compliance on residential ratepayers;

(4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and

(5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

(c) EXTENSION OF COMPLIANCE DATE FOR EQUIPMENT, FACILITIES, AND SERVICES.—

(1) PETITION.—A telecommunications carrier proposing to install or deploy, or having installed or deployed, any equipment, facility, or service prior to the effective date of section 103 may petition the Commission for 1 or more extensions of the deadline for complying with the assistance capability requirements under section 103.

(2) GROUNDS FOR EXTENSION.—The Commission may, after consultation with the Attorney General, grant an extension under this subsection, if the Commission determines that compliance with the assistance capability requirements under section 103 is not reasonably achievable through application of technology available within the compliance period.

(3) LENGTH OF EXTENSION.—An extension under this subsection shall extend for no longer than the earlier of—

(A) the date determined by the Commission as necessary for the carrier to comply with the assistance capability requirements under section 103; or

(B) the date that is 2 years after the date on which the extension is granted.

(4) APPLICABILITY OF EXTENSION.—An extension under this subsection shall apply to only that part of the carrier's business on which the new equipment, facility, or service is used.

SEC. 108. ENFORCEMENT ORDERS.

(a) GROUNDS FOR ISSUANCE.—A court shall issue an order enforcing this title under section 2522 of title 18, United States Code, only if the court finds that—

(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and

(2) compliance with the requirements of this title is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.

(b) TIME FOR COMPLIANCE.—Upon issuing an order enforcing this title, the court shall specify a reasonable time and conditions for complying with its order, considering the good faith efforts to comply in a timely manner, any effect on the carrier's, manufacturer's, or service provider's ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require.

(c) LIMITATIONS.—An order enforcing this title may not—

(1) require a telecommunications carrier to meet the government's demand for interception of communications and acquisition of call-identifying information to any extent in excess of the capacity for which the Attorney General has agreed to reimburse such carrier;

(2) require any telecommunications carrier to comply with assistance capability requirement of section 103 if the Commission has determined (pursuant to section 109(b)(1)) that compliance is not reasonably achievable, unless the Attorney General has agreed (pursuant to section 109(b)(2)) to pay the costs described in section 109(b)(2)(A); or

(3) require a telecommunications carrier to modify, for the purpose of complying with the assistance capability requirements of section 103, any equipment, facility, or service deployed on or before January 1, 1995, unless—

(A) the Attorney General has agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring the equipment, facility, or service into compliance with those requirements; or

(B) the equipment, facility, or service has been replaced or significantly upgraded or otherwise undergoes major modification.

SEC. 109. PAYMENT OF COSTS OF TELECOMMUNICATIONS CARRIERS TO COMPLY WITH CAPABILITY REQUIREMENTS.

(a) EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED ON OR BEFORE JANUARY 1, 1995.—The Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103.

(b) EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED AFTER JANUARY 1, 1995.—

(1) DETERMINATIONS OF REASONABLY ACHIEVABLE.—The Commission, on petition from a telecommunications carrier or any other interested person, and after notice to the Attorney General, shall determine whether compliance with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility, or service installed or deployed

after January 1, 1995. The Commission shall make such determination within 1 year after the date such petition is filed. In making such determination, the Commission shall determine whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems and shall consider the following factors:

(A) The effect on public safety and national security.

(B) The effect on rates for basic residential telephone service.

(C) The need to protect the privacy and security of communications not authorized to be intercepted.

(D) The need to achieve the capability assistance requirements of section 103 by cost-effective methods.

(E) The effect on the nature and cost of the equipment, facility, or service at issue.

(F) The effect on the operation of the equipment, facility, or service at issue.

(G) The policy of the United States to encourage the provision of new technologies and services to the public.

(H) The financial resources of the telecommunications carrier.

(I) The effect on competition in the provision of telecommunications services.

(J) The extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995.

(K) Such other factors as the Commission determines are appropriate.

(2) COMPENSATION.—If compliance with the assistance capability requirements of section 103 is not reasonably achievable with respect to equipment, facilities, or services deployed after January 1, 1995—

(A) the Attorney General, on application of a telecommunications carrier, may agree, subject to the availability of appropriations, to pay the telecommunications carrier for the additional reasonable costs of making compliance with such assistance capability requirements reasonably achievable; and

(B) if the Attorney General does not agree to pay such costs, the telecommunications carrier shall be deemed to be in compliance with such capability requirements.

(c) ALLOCATION OF FUNDS FOR PAYMENT.—The Attorney General shall allocate funds appropriated to carry out this title in accordance with law enforcement priorities determined by the Attorney General.

(d) FAILURE TO MAKE PAYMENT WITH RESPECT TO EQUIPMENT, FACILITIES, AND SERVICES DEPLOYED ON OR BEFORE JANUARY 1, 1995.—If a carrier has requested payment in accordance with procedures promulgated pursuant to subsection (e), and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of section 103, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification.

(e) COST CONTROL REGULATIONS.—

(1) IN GENERAL.—The Attorney General shall, after notice and comment, establish regulations necessary to effectuate timely and cost-efficient payment to telecommunications carriers under this title, under chapters 119 and 121 of title 18, United States Code, and under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(2) CONTENTS OF REGULATIONS.—The Attorney General, after consultation with the Commission, shall prescribe regulations for purposes of determining reasonable costs under this title. Such regulations shall seek to minimize the cost to the Federal Government and shall—

(A) permit recovery from the Federal Government of—

(i) the direct costs of developing the modifications described in subsection (a), of providing the capabilities requested under subsection (b)(2), or of providing the capacities requested under section 104(e), but only to the extent that such costs have not been recovered from any other governmental or nongovernmental entity;

(ii) the costs of training personnel in the use of such capabilities or capacities; and

(iii) the direct costs of deploying or installing such capabilities or capacities;

(B) in the case of any modification that may be used for any purpose other than lawfully authorized electronic surveillance by a law enforcement agency of a government, permit recovery of only the incremental cost of making the modification suitable for such law enforcement purposes; and

(C) maintain the confidentiality of trade secrets.

(3) SUBMISSION OF CLAIMS.—Such regulations shall require any telecommunications carrier that the Attorney General has agreed to pay for modifications pursuant to this section and that has installed or deployed such modification to submit to the Attorney General a claim for payment that contains or is accompanied by such information as the Attorney General may require.

SEC. 110. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this title a total of $500,000,000 for fiscal years 1995, 1996, 1997, and 1998. Such sums are authorized to remain available until expended.

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title shall take effect on the date of enactment of this Act.

(b) ASSISTANCE CAPABILITY AND SYSTEMS SECURITY AND INTEGRITY REQUIREMENTS.—Sections 103 and 105 of this title shall take effect on the date that is 4 years after the date of enactment of this Act.

SEC. 112. REPORTS.

(a) REPORTS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—On or before November 30, 1995, and on or before November 30 of each year thereafter, the Attorney General shall submit to Congress and make available to the public a report on the amounts paid during the preceding fiscal year to telecommunications carriers under sections 104(e) and 109.

(2) CONTENTS.—A report under paragraph (1) shall include—

(A) a detailed accounting of the amounts paid to each carrier and the equipment, facility, or service for which the amounts were paid; and

(B) projections of the amounts expected to be paid in the current fiscal year, the carriers to which payment is expected to be made, and the equipment, facilities, or services for which payment is expected to be made.

(b) REPORTS BY THE COMPTROLLER GENERAL.—

(1) PAYMENTS FOR MODIFICATIONS.—On or before April 1, 1996, and every 2 years thereafter, the Comptroller General of the United States, after consultation with the Attorney General and the telecommunications industry, shall submit to the Congress a report—

(A) describing the type of equipment, facilities, and services that have been brought into compliance under this title; and

(B) reflecting its analysis of the reasonableness and cost-effectiveness of the payments made by the Attorney General to telecommunications carriers for modifications necessary to ensure compliance with this title.

(2) COMPLIANCE COST ESTIMATES.—A report under paragraph (1) shall include the findings and conclusions of the Comptroller General on the costs to be incurred by telecommunications carriers to comply with the assistance capability requirements of section 103 after the effective date of such section 103, including projections of the amounts expected to be incurred and a description of the equipment, facilities, or services for which they are expected to be incurred.

TITLE II—AMENDMENTS TO TITLE 18, UNITED STATES CODE

SEC. 201. COURT ENFORCEMENT OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT.

(a) COURT ORDERS UNDER CHAPTER 119.—Chapter 119 of title 18, United States Code, is amended by inserting after section 2521 the following new section:

"§ 2522. Enforcement of the Communications Assistance for Law Enforcement Act.

"(a) ENFORCEMENT BY COURT ISSUING SURVEILLANCE ORDER.—If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

"(b) ENFORCEMENT UPON APPLICATION BY ATTORNEY GENERAL.—The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

"(c) CIVIL PENALTY.—

"(1) IN GENERAL.—A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

"(2) CONSIDERATIONS.—In determining whether to impose a civil penalty and in determining its amount, the court shall take into account—

"(A) the nature, circumstances, and extent of the violation;

"(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

"(C) such other matters as justice may require.

"(d) DEFINITIONS.—As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.".

(b) CONFORMING AMENDMENTS.—

(1) Section 2518(4) of title 18, United States Code, is amended by adding at the end the

following new sentence: "Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.".

(2) Section 3124 of such title is amended by adding at the end the following new subsection:

"(f) COMMUNICATIONS ASSISTANCE ENFORCEMENT ORDERS.—Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.".

(3) The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by inserting after the item pertaining to section 2521 the following new item:

"2522. Enforcement of the Communications Assistance for Law Enforcement Act.".

SEC. 202. CORDLESS TELEPHONES.

(a) DEFINITIONS.—Section 2510 of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ", but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (12), by striking subparagraph (A) and redesignating subparagraphs (B), (C), and (D) as subparagraphs (A), (B), and (C), respectively.

(b) PENALTY.—Section 2511 of title 18, United States Code, is amended—

(1) in subsection (4)(b)(i) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

SEC. 203. RADIO-BASED DATA COMMUNICATIONS.

Section 2510(16) of title 18, United States Code, is amended—

(1) by striking "or" at the end of subparagraph (D);

(2) by inserting "or" at the end of subparagraph (E); and

(3) by inserting after subparagraph (E) the following new subparagraph:

"(F) an electronic communication;"

SEC. 204. PENALTIES FOR MONITORING RADIO COMMUNICATIONS THAT ARE TRANSMITTED USING MODULATION TECHNIQUES WITH NONPUBLIC PARAMETERS.

Section 2511(4)(b) of title 18, United States Code, is amended by striking "or encrypted, then" and inserting ", encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then".

SEC. 205. TECHNICAL CORRECTION.

Section 2511(2)(a)(i) of title 18, United States Code, is amended by striking "used in the transmission of a wire communication" and inserting "used in the transmission of a wire or electronic communication".

SEC. 206. FRAUDULENT ALTERATION OF COMMERCIAL MOBILE RADIO INSTRUMENTS.

(a) OFFENSE.—Section 1029(a) of title 18, United States Code, is amended—

(1) by striking "or" at the end of paragraph (3); and

(2) by inserting after paragraph (4) the following new paragraphs:

"(5) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or

"(6) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses—

"(A) a scanning receiver; or

"(B) hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services,".

(b) PENALTY.—Section 1029(c)(2) of title 18, United States Code, is amended by striking "(a)(1) or (a)(4)" and inserting "(a) (1), (4), (5), or (6)".

(c) DEFINITIONS.—Section 1029(e) of title 18, United States Code, is amended—

(1) in paragraph (1) by inserting "electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier," after "account number,";

(2) by striking "and" at the end of paragraph (5);

(3) by striking the period at the end of paragraph (6) and inserting "; and"; and

(4) by adding at the end the following new paragraph:

"(7) the term 'scanning receiver' means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119.".

SEC. 207. TRANSACTIONAL DATA.

(a) DISCLOSURE OF RECORDS.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (c)(1)—

(A) in subparagraph (B)—

(i) by striking clause (i); and

(ii) by redesignating clauses (ii), (iii), and (iv) as clauses (i), (ii), and (iii), respectively; and

(B) by adding at the end the following new subparagraph:

"(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B)."; and

(2) by amending the first sentence of subsection (d) to read as follows: "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3126(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.".

(b) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 3121 of title 18, United States Code, is amended—

(1) by redesignating subsection (c) as subsection (d); and

(2) by inserting after subsection (b) the following new subsection:

"(c) LIMITATION.—A government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.".

SEC. 208. AUTHORIZATION FOR ACTING DEPUTY ATTORNEYS GENERAL IN THE CRIMINAL DIVISION TO APPROVE CERTAIN COURT APPLICATIONS.

Section 2516(1) of title 18, United States Code, is amended by inserting "or acting Deputy Assistant Attorney General" after "Deputy Assistant Attorney General".

TITLE III—AMENDMENTS TO THE COMMUNICATIONS ACT OF 1934

SEC. 301. COMPLIANCE COST RECOVERY.

Title II of the Communications Act of 1934 is amended by inserting after section 228 (47 U.S.C. 228) the following new section:

"SEC. 229. COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT COMPLIANCE.

"(a) IN GENERAL.—The Commission shall prescribe such rules as are necessary to implement the requirements of the Communications Assistance for Law Enforcement Act.

"(b) SYSTEMS SECURITY AND INTEGRITY.—The rules prescribed pursuant to subsection (a) shall include rules to implement section 105 of the Communications Assistance for Law Enforcement Act that require common carriers—

"(1) to establish appropriate policies and procedures for the supervision and control of its officers and employees—

"(A) to require appropriate authorization to activate interception of communications or access to call-identifying information; and

"(B) to prevent any such interception or access without such authorization;

"(2) to maintain secure and accurate records of any interception or access with or without such authorization; and

"(3) to submit to the Commission the policies and procedures adopted to comply with the requirements established under paragraphs (1) and (2).

"(c) COMMISSION REVIEW OF COMPLIANCE.—The Commission shall review the policies and procedures submitted under subsection (b)(3) and shall order a common carrier to modify any such policy or procedure that the Commission determines does not comply with Commission regulations. The Commission shall conduct such investigations as may be necessary to insure compliance by common carriers with the requirements of the regulations prescribed under this section.

"(d) PENALTIES.—For purposes of this Act, a violation by an officer or employee of any policy or procedure adopted by a common carrier pursuant to subsection (b), or of a rule prescribed by the Commission pursuant to subsection (a), shall be considered to be a violation by the carrier of a rule prescribed by the Commission pursuant to this Act.

"(e) COST RECOVERY FOR COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT COMPLIANCE.—

"(1) PETITIONS AUTHORIZED.—A common carrier may petition the Commission to adjust charges, practices, classifications, and regulations to recover costs expended for making modifications to equipment, facilities, or services pursuant to the requirements of section 103 of the Communications Assistance for Law Enforcement Act.

"(2) COMMISSION AUTHORITY.—The Commission may grant, with or without modification, a petition under paragraph (1) if the Commission determines that such costs are reasonable and that permitting recovery is consistent with the public interest. The Commission may, consistent with maintaining just and reasonable charges, practices, classifications, and regulations in connection with the provision of interstate or foreign communication by wire or radio by a common carrier, allow carriers to adjust such charges, practices, classifications, and regulations in order to carry out the purposes of this Act.

"(3) JOINT BOARD.—The Commission shall convene a Federal-State joint board to recommend appropriate changes to part 36 of the Commission's rules with respect to recovery of costs pursuant to charges, practices, classifications, and regulations under the jurisdiction of the Commission.".

SEC. 302. RECOVERY OF COST OF COMMISSION PROCEEDINGS.

The schedule of application fees in section 8(g) of the Communications Act of 1934 (47 U.S.C. 158(g)) is amended by inserting under item 1 of the matter pertaining to common carrier services the following additional subitem:

"d. Proceeding under section 109(b) of the Communications Assistance for Law Enforcement Act .... 5,000".

SEC. 303. CLERICAL AND TECHNICAL AMENDMENTS.

(a) AMENDMENTS TO THE COMMUNICATIONS ACT OF 1934.—The Communications Act of 1934 is amended—

(1) in section 4(f)(3), by striking "overtime exceeds beyond" and inserting "overtime extends beyond";

(2) in section 5, by redesignating subsection (f) as subsection (e);

(3) in section 8(d)(2), by striking "payment of a" and inserting "payment of an";

(4) in the schedule contained in section 8(g), in item 7.f. under the heading "EQUIPMENT APPROVAL SERVICES/EXPERIMENTAL RADIO" by striking "Additional Charge" and inserting "Additional Application Fee";

(5) in section 9(f)(1), by inserting before the second sentence the following:

"(2) INSTALLMENT PAYMENTS.—";

(6) in the schedule contained in section 9(g), in the item pertaining to interactive video data services under the private radio bureau, insert "95" after "47 C.F.R. Part";

(7) in section 220(a)—

(A) by inserting "(1)" after "(a); and

(B) by adding at the end the following new paragraph:

"(2) The Commission shall, by rule, prescribe a uniform system of accounts for use by telephone companies. Such uniform system shall require that each common carrier shall maintain a system of accounting methods, procedures, and techniques (including accounts and supporting records and memoranda) which shall ensure a proper allocation of all costs to and among telecommunications services, facilities, and products (and to and among classes of such services, facilities, and products) which are developed, manufactured, or offered by such common carrier.";

(8) in section 220(b), by striking "clasess" and inserting "classes";

(9) in section 223(b)(3), by striking "defendant restrict access" and inserting "defendant restricted access";

(10) in section 226(d), by striking paragraph (2) and redesignating paragraphs (3) and (4) as paragraphs (2) and (3), respectively;

(11) in section 227(b)(2)(C), by striking "paragraphs" and inserting "paragraph";

(12) in section 227(e)(2), by striking "national datebase" and inserting "national database";

(13) in section 228(c), by redesignating the second paragraph (2) and paragraphs (3) through (6) as paragraphs (3) through (7), respectively;

(14) in section 228(c)(6)(D), by striking "conservation" and inserting "conversation";

(15) in section 308(c), by striking "May 24, 1921" and inserting "May 27, 1921";

(16) in section 309(c)(2)(F), by striking "section 325(b)" and inserting "section 325(c)";

(17) in section 309(i)(4)(A), by striking "Communications Technical Amendments Act of 1982" and inserting "Communications Amendments Act of 1982";

(18) in section 331, by amending the heading of such section to read as follows:

"VERY HIGH FREQUENCY STATIONS AND AM RADIO STATIONS";

(19) in section 358, by striking "(a)";

(20) in part III of title III—

(A) by inserting before section 381 the following heading:

"VESSELS TRANSPORTING MORE THAN SIX PASSENGERS FOR HIRE REQUIRED TO BE EQUIPPED WITH RADIO TELEPHONE";

(B) by inserting before section 382 the following heading:

"VESSELS EXCEPTED FROM RADIO TELEPHONE REQUIREMENT";

(C) by inserting before section 383 the following heading:

"EXEMPTIONS BY COMMISSION";

(D) by inserting before section 384 the following heading:

"AUTHORITY OF COMMISSION; OPERATIONS, INSTALLATIONS, AND ADDITIONAL EQUIPMENT";

(E) by inserting before section 385 the following heading:

"INSPECTIONS"; and

(F) by inserting before section 386 the following heading:

"FORFEITURES";

(21) in section 410(c), by striking ", as referred to in sections 202(b) and 205(f) of the Interstate Commerce Act,";

(22) in section 613(b)(2), by inserting a comma after "pole" and after "line";

(23) in section 624(d)(2)(A), by inserting "of" after "viewing";

(24) in section 634(h)(1), by striking "section 602(6)(A)" and inserting "section 602(7)(A)";

(25) in section 705(d)(6), by striking "subsection (d)" and inserting "subsection (e)";

(26) in section 705(e)(3)(A), by striking "paragraph (4) of subsection (d)" and inserting "paragraph (4) of this subsection";

(27) in section 705, by redesignating subsections (f) and (g) (as added by Public Law 100-667) as subsections (g) and (h); and

(28) in section 705(h) (as so redesignated), by striking "subsection (f)" and inserting "subsection (g)".

(b) AMENDMENTS TO THE COMMUNICATIONS SATELLITE ACT OF 1962.—The Communications Satellite Act of 1962 is amended—

(1) in section 303(a)—

(A) by striking "section 27(d)" and inserting "section 327(d)";

(B) by striking "sec. 29-911(d)" and inserting "sec. 29-327(d)";

(C) by striking "section 36" and inserting "section 336"; and

(D) by striking "sec. 29-916d" and inserting "section 29-336(d)";

(2) in section 304(d), by striking "paragraphs (1), (2), (3), (4), and (5) of section 310(a)" and inserting "subsection (a) and paragraphs (1) through (4) of subsection (b) of section 310"; and

(3) in section 304(e)—

(A) by striking "section 45(b)" and inserting "section 345(b)"; and

(B) by striking "sec. 29-920(b)" and inserting "sec. 29-345(b)"; and

(4) in sections 502(b) and 503(a)(1), by striking "the Communications Satellite Corporation" and inserting "the communications satellite corporation established pursuant to title III of this Act".

(c) AMENDMENT TO THE CHILDREN'S TELEVISION ACT OF 1990.—Section 103(a) of the Children's Television Act of 1990 (47 U.S.C. 303b(a)) is amended by striking "noncommerical" and inserting "noncommercial".

(d) AMENDMENTS TO THE TELECOMMUNICATIONS AUTHORIZATION ACT OF 1992.—Section 205(1) of the Telecommunications Authorization Act of 1992 is amended—

(1) by inserting an open parenthesis before "other than"; and

(2) by inserting a comma after "stations)".

(e) CONFORMING AMENDMENT.—Section 1253 of the Omnibus Budget Reconciliation Act of 1981 is repealed.

(f) STYLISTIC CONSISTENCY.—The Communications Act of 1934 and the Communications Satellite Act of 1962 are amended so that the section designation and section heading of each section of such Acts shall be in the form and typeface of the section designation and heading of this section.

SEC. 304. ELIMINATION OF EXPIRED AND OUTDATED PROVISIONS.

(a) AMENDMENTS TO THE COMMUNICATIONS ACT OF 1934.—The Communications Act of 1934 is amended—

(1) in section 7(b), by striking "or twelve months after the date of the enactment of this section, if later" both places it appears;

(2) in section 212, by striking "After sixty days from the enactment of this Act it shall" and inserting "It shall";

(3) in section 213, by striking subsection (g) and redesignating subsection (h) as subsection (g);

(4) in section 214, by striking "section 221 or 222" and inserting "section 221";

(5) in section 220(b), by striking ", as soon as practicable,";

(6) by striking section 222;

(7) in section 224(b)(2), by striking "Within 180 days from the date of enactment of this section the Commission" and inserting "The Commission";

(8) in 226(e), by striking "within 9 months after the date of enactment of this section,";

(9) in section 309(i)(4)(A), by striking "The commission, not later than 180 days after the date of the enactment of the Communications Technical Amendments Act of 1982, shall," and inserting "The Commission shall,";

(10) by striking section 328;

(11) in section 413, by striking ", within sixty days after the taking effect of this Act,";

(12) in section 624(d)(2)(B)—

(A) by striking out "(A)";

(B) by inserting "of" after "restrict the viewing"; and

(C) by striking subparagraph (B);

(13) by striking sections 702 and 703;

(14) in section 704—

(A) by striking subsections (b) and (d); and

(B) by redesignating subsection (c) as subsection (b);

(15) in section 705(g) (as redesignated by section 304(25)), by striking "within 6 months after the date of enactment of the Satellite Home Viewer Act of 1988, the Federal Communications Commission" and inserting "The Commission";

(16) in section 710(f)—

(A) by striking the first and second sentences; and

(B) in the third sentence, by striking "Thereafter, the Commission" and inserting "The Commission";

(17) in section 712(a), by striking ", within 120 days after the effective date of the Satellite Home Viewer Act of 1988,"; and

(18) by striking section 713.

(b) AMENDMENTS TO THE COMMUNICATIONS SATELLITE ACT OF 1962.—The Communications Satellite Act of 1962 is amended—

(1) in section 201(a)(1), by striking "as expeditiously as possible,";

(2) by striking sections 301 and 302 and inserting the following:

"SEC. 301. CREATION OF CORPORATION.

"There is authorized to be created a communications satellite corporation for profit which will not be an agency or establishment of the United States Government.

"SEC. 302. APPLICABLE LAWS.

"The corporation shall be subject to the provisions of this Act and, to the extent consistent with this Act, to the District of Columbia Business Corporation Act. The right to repeal, alter, or amend this Act at any time is expressly reserved.";

(3) in section 304(a), by striking "at a price not in excess of $100 for each share and";

(4) in section 404—

(A) by striking subsections (a) and (c); and

(B) by redesignating subsection (b) as section 404;

(5) in section 503—

(A) by striking paragraph (2) of subsection (a); and

(B) by redesignating paragraph (3) of subsection (a) as paragraph (2) of such subsection;

(C) by striking subsection (b);

(D) in subsection (g)—

(i) by striking "subsection (c)(3)" and inserting "subsection (b)(3)"; and

(ii) by striking the last sentence; and

(E) by redesignating subsections (c) through (h) as subsections (b) through (g), respectively;

(5) by striking sections 505, 506, and 507; and

(6) by redesignating section 508 as section 505.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas [Mr. BROOKS] will be recognized for 20 minutes, and the gentleman from Illinois [Mr. HYDE] will be recognized for 20 minutes.

The Chair recognizes the gentleman from Texas [Mr. BROOKS].

Mr. BROOKS. Mr. Speaker, I yield myself such time as I may consume.

(Mr. BROOKS asked and was given permission to revise and extend his remarks, and to include extraneous material.)

Mr. BROOKS. Mr. Speaker, H.R. 4922 specifies a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes. It is the result of extensive negotiations among law enforcement, Congress, industry and the privacy community. I applaud DON EDWARDS, the chairman of the Subcommittee on Civil and Constitutional Rights, ranking Member HENRY HYDE and JOHN DINGELL, chairman of the Committee on Energy and Commerce, for helping to craft a bill that these diverse interests can live with. It is essential that we support the very real law enforcement objectives at the heart of the legislation without minimizing industry's legitimate concerns regarding both privacy protections and costs resulting from installing new technology to this end, the bill laudably protects public safety by requiring telecommunications carriers to be able to fulfill court authorized requests for interceptions without overreaching into protected privacy areas. At the same time, it requires law enforcement to pay retrofitting costs necessary to start up this legislation—up to $500 million over the next 4 years. Beyond that, carriers will only be required to incur reasonable costs to comply with the bill.

I want to be very clear on one point: While there is no way Government can pay the costs of new technology associated with law enforcement wiretapping needs in perpetuity, I also believe that industry must receive fair reimbursement for some of their research, development, and start-up costs. Beyond that period of time, an equitable arrangement between Government and private industry must be reached. The proposal before the House is a tremendous improvement over prior treatment of this issue.

Finally, it is also worth noting that this bill does not expand law enforcement authority to conduct these interceptions. In fact, the bill includes several provisions to improve the privacy and security in the telecommunications network.

This is a good balance, and a good bill. I urge my colleagues to pass this important legislation.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, October 4, 1994.

Hon. JACK BROOKS,
Chairman, Committee on the Judiciary, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I am writing with respect to H.R. 4922, which was ordered reported by the Committee on the Judiciary on September 29. As you know, I have written to the Speaker protesting the initial referral solely to the Committee on the Judiciary, and asking that the Committee on Energy and Commerce receive an extended sequential referral once the Committee on the Judiciary has filed its report. Enclosed please find a copy of that letter for your reference.

Since that time, the Committee staff (both majority and minority) have been working with your staff to attempt to resolve the problems articulated in the letter. They have succeeded in crafting a compromise which addresses our jurisdictional concerns, while preserving the essential elements of H.R. 4922 as it was ordered reported by your Committee.

Specifically, the legislation has been redrafted and reorganized to separate provisions that fall within the jurisdiction of both of our committees from those which fall exclusively within the jurisdiction of one or the other. Title I of the text creates a freestanding statute that is not codified, which governs the interception of digital and other communications transmitted by telecommunications carriers. This Title imposes new regulations on communications carriers, a subject which is expressly part of our Committee's Rule X jurisdiction. In my view, it ought to be codified in Title 47 of the U.S. Code, which is where other matters of this sort are codified.

However, this Title also implicates the law enforcement jurisdiction of the Committee on the Judiciary. In recognition of your legitimate claim for jurisdiction, in my view jurisdiction over this Title should be shared by our two committees.

Title II amends Title 18 and falls exclusively within the jurisdiction of the Committee on the Judiciary.

Title III amends the Communications Act of 1934 and falls exclusively within the jurisdictions of the Committee on Energy and Commerce.

Our Committee intends to insist on its request for sequential referral. However, in light of the agreement that has been reached by our two committees, and subject to it being offered during the House consideration of the bill, the Committee on Energy and Commerce will not object to the consideration of H.R. 4922 by the full House later today. I do ask, however, that you insert a copy of this letter, together with your response, into the Record during floor consideration.

Sincerely,

JOHN D. DINGELL, *Chairman.*

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, October 4, 1994.

Hon. JOHN D. DINGELL,
Chairman, Committee on Energy and Commerce, Rayburn House Office Building, Washington, DC.

DEAR JOHN: I am writing in response to your correspondence dated October 4, 1994, regarding H.R. 4992, legislation to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes.

As you know, our Committees have worked closely on this legislation to address areas of common concern. I very much appreciate your strong leadership and the efforts of other Members of the Committee on Energy and Commerce in working to craft a mutually agreeable legislative product that serves to maximize the protection of various law enforcement, privacy and commercial interests.

I acknowledge that the bill, as ordered reported by the Committee on the Judiciary, contains some subject matter within the Rule X jurisdiction of your Committee that would render an appropriate referral of the legislation at this time. I very much appreciate your willingness to allow the House later today to consider H.R. 4922, as modified pursuant to the discussions between our Committees. I further concur with the comments in your letter regarding the division of jurisdiction in the three titles of the legislation to be considered today.

Meanwhile, with best wishes.

Sincerely,

JACK BROOKS, *Chairman.*

Mr. Speaker, I reserve the balance of my time.

Mr. HYDE. Mr. Speaker, I yield myself such time as I may consume.

(Mr. HYDE asked and was given permission to revise and extend his remarks.)

Mr. HYDE. Mr. Speaker, this legislation, which represents a joint effort by the Committee on the Judiciary and the Committee on Energy and Commerce, is needed to insure that technological advances in the telecommunications industry do not foreclose the ability of law enforcement to conduct court—authorized electronic surveillance. I am pleased to have been an original co-sponsor of this legislation with the chairman of the Subcommittee on Civil on Constitutional Rights, Mr. EDWARDS.

H.R. 4922, as amended seeks to carefully balance the needs of law enforcement, the interests of the telecommunications industry and the privacy rights of the American public in order to insure that law enforcement can continue to conduct court-authorized wiretaps.

Earlier this year, the Subcommittee on Civil and Constitutional Rights held two joint hearings with the Senate

Subcommittee on Technology and the Law. Our hearings revealed that obstacles to court-authorized interceptions are already being encountered. An informal survey conducted by the FBI of Federal, State, and local law enforcement agencies in April of this year revealed 183 technology-based problems encountered in attempts to conduct court-authorized electronic surveillance.

The bill makes it clear that all telecommunications carriers will cooperate and assist in the interception of communications for law enforcement purposes. the definition of "telecommunications carrier" includes such service providers as local exchange carriers, interexchange carriers, competitive access providers [CAPs], cellular carriers, providers of personal communications services (PCS), satellite-based service providers, cable operators, and electric and other utilities that provide telecommunications services for hire to the public, and any other wireline or wireless service for hire to the public.

The bill authorizes an appropriation of $500 million for fiscal years 1995 through 1998, and for subsequent years, such sums as are necessary for telecommunications carriers to retrofit existing facilities to bring them into compliance with law enforcement requirements.

Those covered by the bill have expressed concern that $500 million will not cover the cost of retrofitting existing facilities. Because we do not yet know the exact nature of the technologies that will be needed to satisfy the capability requirements, we cannot know, with certainty, exactly how much money will be needed to retrofit existing services and facilities. According to the GAO, "until capability solutions and capacity requirements are better defined, it is virtually impossible to project a precise estimate of the reimbursement costs of this bill."

If the $500 million authorized in the bill is not appropriated, or if it not sufficient to cover retrofit costs, any equipment or services that the government cannot pay to retrofit are "grandfathered," and do not have to be brought into compliance until they are replaced or upgraded in the ordinary course of business.

After the 4 year transition period, which may be extended up to two additional years by order of the FCC, industry will pay to insure that new equipment and services meet the legislative requirements as defined by industry standards and specifications to the extent such compliance is reasonably achievable. In the event that compliance is not reasonably achievable, a telecommunications carrier may petition the FCC to determine whether costs of compliance would impose significant difficulty or expense based on 10 enumerated factors including public safety and national security, the impact on rates for basic residential telephone service and the like. If compliance is not reasonably achievable, and the Attorney General does not agree to reimburse, the carrier will not be required to pay to bring its services or features into compliance.

In addition, to the extent that telecommunications carriers must install additional capacity to meet law enforcement needs, the bill requires the Government to pay for the increased capacity requirements.

Court authorized electronic surveillance is one of law enforcement's most important and effective investigative tools. It is often the only means of preventing or solving serious crimes. Failure to pass this legislation will have dire consequences for law enforcement, public safety and our national security.

This legislation is strongly supported by FBI Director Freeh and State and local law enforcement officials. I urge my colleagues to do so as well.

Mr. Speaker, I reserve the balance of my time.

Mr. BROOKS. Mr. Speaker, I yield 3 minutes to the distinguished gentleman from Massachusetts [Mr. MARKEY].

Mr. MARKEY. Mr. Speaker, I rise in support of H.R. 4922, which makes certain that law enforcement's needs for wiretaps are met as we march forward into the future.

This bill seeks to balance the growth of the communications industry and its advances in technology, something my Subcommittee has taken pains to promote, with the legitimate needs of law enforcement for wiretap capabilities.

The issue of wiretapping telephone lines has dogged constitutional, privacy, and telecommunications advocates for decades. In fact, wiretap law reflects a 65-year history between Congress and the courts. In 1928, the Supreme Court first confronted the issue in Olmstead v United States. In this famous case, the Court held that tapping a telephone line does not constitute a "search" or "seizure" and therefore does not violate the Fourth Amendment. This case is most famous, however, for the dissent by Justice Brandeis, who argued that the Constitution protected citizens against wiretaps. In that great Justice's most memorable phrase, he wrote that:

> The Fourth Amendment protected against wiretaps because it protected the right of privacy, which he defined as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."

Congress responded to the Court's decision in Olmstead, and the force of Justice Brandeis' dissent, just 6 years later. In passing the Communications Act of 1934, Congress included a provision in section 705, that states "no person not being authorized by the sender shall intercept any communication and divulge or publish [its] existence, contents * * * or meaning." However, courts quickly construed section 705 to permit Federal and State law enforcement to use a wiretap for investigation purposes, so long as they did not divulge any content by testifying about it in open court.

Then, in 1967, the Supreme Court finally adopted Justice Brandeis' dissenting view, overruled Olmstead, and held that an eavesdropping does amount to a "search or seizure" and thus was protected by the Constitution. Just 1 year later, Congress again responded, by passing the 1968 Wiretap Act. This law makes wiretaps lawful by setting up a judicial process that law enforcement must go through to get a court-ordered wiretap.

But the story does not end there Congress again responded to changes in computer and communications technology by passing the Electronic Communications Privacy Act of 1986. This law, which was sponsored by Senator LEAHY and Congressman EDWARDS, amended the 1968 Wiretap Act by protecting a new class of electronic communications, defined broadly to include everything from e-mail to databases. That legislation reflected an ongoing effort to update and clarify Federal wiretap laws, as the Senate Committee put it, "in light of dramatic changes in new computer and telecommunications technologies."

Well today, we are back at the task of updating and clarifying our wiretap law again. This time, the changes in computer and telecommunications technology are not just dramatic, they are overwhelming. The growth of digital communications over the past 8 years, the spread of fiber deeper into the local phone network, the spread and growth of wireless services—all of these developments converge to compel us to address legislatively the needs of law enforcement in the information age. The Federal Bureau of Investigation argues that as these advanced technologies get deployed, that the technology should not, in essence, repeal or modify the 1968 Wiretap Act. Instead, the Bureau argues, we must update and clarify our laws so that their ability to conduct wiretaps is maintained—not expanded and not diminished—just maintained.

In working with the Judiciary Committee to resolve this matter, I have sought to come up with a policy that 1) protects the privacy interests of our citizens, 2) is mindful of the limited financial resources of taxpayers or ratepayers, 3) meets the legitimate needs of law enforcement, and 4) does not unduly interfere with our telecommunications industry, which is racing to the future with advances in communications technology.

The bill before the House today, carefully crafted in consultation between our two committees, represents a balanced and workable approach to resolving each of those issues. I urge the House to approve this bill.

In addition, I want to comment in detail on several provisions in the bill. The term "information services" encompasses both electronic publishing, which has meaning under the MFJ and FCC and court interpretations, and electronic messaging services, which is a term broadly defined to encompass electronic mail, electronic forms transfer, electronic document interchange, and electronic data interchange. The term "telecommunications carrier" is not a defined term in the Communications Act of 1934, but the term is defined broadly to include common carriers, which means, at minimum both a "common carrier," as defined in section 3(h), and a provider of "telephone exchange service," as such term is defined in section 3(r). Consequently, all local exchange carriers and long distance companies operating as common carriers will be covered. In addition, the provision in (4)(B)(ii) applies to persons or entities that offer a service that represents a substantial substitute for a common carrier service. This provision, coupled with the language in (4)(A), is designed to sweep broadly. However, in recognition that not all common carriers need to be covered by this Act, and in recognition that law enforcement does not need capability assistance from all carriers, the legislation also directs the Commission, in paragraph (8)(C)(ii), to exclude certain carriers.

Section 104 requires the Attorney General to publish in the Federal Register notice of the actual capacity and maximum capacity that law enforcement will need from telecommunications carriers. Section 104(a)(2) requires the Attorney General to identify capacity required at specific locations, and to base the notice on the type of equipment or service involved, or the kind or type of carrier. The purpose behind this provision is two-fold. One, to ensure that carriers receive adequate and specific notice from the Attorney General about the needs of law enforcement with respect to a particular carrier in a particular area. This notice is essential to enable a carrier to meet its obligations under section 104(d). Second, this provision encourages the Attorney General to recognize differences among telecommunications carriers, and to take those differences into account when issuing a notice.

Section 105 represents a significant expansion of privacy protection for citizens everywhere. It ensures that wiretapping technology does not become so easy as to obviate the need for telephone company participation, which serves as a check against an end-run of the judicial system. The Energy and Commerce Committee found this interest so compelling, that in title III of the bill we direct the Federal Communications Commission to adopt special rules to enforce this requirement, and to have companies submit their procedures for safeguarding those rules with the Commission so that this preventive measure is subject to public notice and not diluted.

Section 109 establishes the principle that for equipment or facilities or services deployed on or before the date of enactment, that the Attorney General, subject to the availability of appropriations, may agree to compensate carriers for all reasonable cost directly associated with necessary modifications to bring equipment, facilities, or services into compliance with the capabilities requirements set forth in section 103. Section 109(b) sets forth the rule for equipment, facilities, or services deployed after the date of enactment. The Commission is directed to determine, upon a petition from a carrier or a manufacturer or any other interested party, whether compliance with section 103 is reasonably achievable for equipment deployed after the date of enactment. The legislation, in turn, elaborates on reasonably achievable as meaning whether compliance would impose significant difficulty or expense.

Section 109(b)(1) lists several factors the Commission should consider in determining whether compliance is reasonably achievable. Those factors direct the Commission's attention to, inter alia, the impact on rates for basic residential telephone service, the need to protect privacy interests, the need to meet law enforcement's needs in a cost-effective manner, the policy of the United States to encourage development and deployment of new technologies and services, and the competitive impact that compliance will have on the offering of the equipment, facilities, or services. These factors are designed to give the Commission direction so that the following goals are realized: (1) Costs to consumers are kept low, so that "gold-plating" by the industry is kept in check; (2) the legitimate needs of law enforcement are met, but that law enforcement does not engage in "gold-plating" of its demands; (3) privacy interests of all Americans are protected; (4) the goal of encouraging competition in all forms of telecommunications is not undermined, and the fact of wiretap compliance is not used as either a sword or a shield in realization of that goal.

Section 109(e) also directs the Attorney General to promulgate regulations designed to minimize the costs to the Federal Government. These regulations serve the purpose of enabling the Attorney General to assess fairly the expenses incurred by carriers, and to reimburse them accordingly.

In administering the rulemaking duties under this Act, the Commission, and the Attorney General, must be careful to protect the genuine proprietary concerns of manufacturers and carriers. (By genuine I mean information that the agency beliefs would present a harm to the competitive position of a company if released.) The proceedings required by this Act may necessitate carriers and manufacturers to file proprietary information which, if disclosed, could affect adversely the competitive position of the company or service at issue. The Commission has procedures in place, under 47 CFR 0.459, .461, to honor requests for confidentiality and to grant review of confidential documents on a limited and protected basis. The Commission should make use of these procedures so that all parties, including public interest and privacy advocates, can have access to the information, but that such information is handled pursuant to strict guidelines. The practice at the U.S. Trade Representative to handle dumping cases is generally acknowledged as workable and well administered. The Commission, and the Attorney General, should seek to establish similar rules to handle genuine proprietary information.

Title III amends the Communications Act of 1934 by requiring the Commission to promulgate rules enforcing the Communications Assistance for Law Enforcement Act in accordance with its Communications Act, title II, regulations. This provision in new section 229(a), coupled with the systems security and integrity provisions in subsections (b) and (c), and the penalties and enforcement provisions in subsection (d), ensures that the Commission will be able to enforce the security, privacy, and cost-effective rules mandated by this Act.

Finally, title III contains a long list of technical corrections and clerical amendments. These amendments are the definition of technical amendments—spelling errors and bad references—but are a necessary step from time to time.

□ 2040

Mr. Speaker, I congratulate the gentleman from Texas, Chairman BROOKS, the gentleman from Michigan, [Mr. DINGELL], especially the gentleman from California, [Mr. EDWARDS], and Senator LEAHY, who have made today's legislation possible.

Mr. HYDE. Mr. Speaker, I yield three minutes to the distinguished gentleman from Texas, [Mr. FIELDS].

(Mr. FIELDS of Texas asked and was given permission to revise and extend his remarks.)

Mr. FIELDS of Texas. Mr. Speaker, I rise in support of H.R. 4922, a bill to amend title 18, U.S. Code, regarding the interception of communications for law enforcement purposes. This bill represents the hard work of many Energy and Commerce and Judiciary Committee members over the past several months. I want to command Mr. EDWARDS, in particular, for his leadership role on this issue.

This legislation is necessary because advancements in technology that have modernized our national telecommunications network at a pace that has outstripped the ability of law enforcement to carry out its law enforcement obligations under Federal wiretap laws. Specifically, new features such as call forwarding, three-way conferencing, and voice recognition calling have made it impossible for wiretaps to be conducted.

I should note that I have never witnessed Federal, State, and local law enforcement officials so united on the need for passage of a legislative proposal. I have heard from officials at all three levels and I specifically want to commend FBI Director Freeh for his hard work on this legislation and Sheriff Klevenhagers of Houston. I also want to complement the telephone industry and the privacy community for their important contributions to this legislation.

This bill will compensate telephone companies for retrofitting their networks to allow law enforcement to conduct authorized wiretaps in light of currently available telephone features and services. In the future, as new technologies come on line, the telephone industry will be responsible for making sure that wiretaps may be conducted. The bill asks the FCC to determine whether the costs are reasonably achievable, and if they are not, we will need to seek Federal funding to pay for the network changes necessary.

I again want to commend the sponsor, Mr. EDWARDS, and Messrs. DINGELL, MOORHEAD, BROOKS, FISH, HYDE, MARKEY, BOUCHER, and OXLEY for their hard work on this matter.

Mr. BROOKS. Mr. Speaker, I yield 3 minutes to the distinguished gentleman from California, [Mr. EDWARDS] chairman of the subcommittee who has done so much to craft this legislation and who is going to be retiring this year, and who we will not be able to replace. We will get a new Member, but he will never replace DON EDWARDS.

Mr. EDWARDS of California. Mr. Speaker, I thank my chairman for those gracious remarks.

(Mr. EDWARDS of California asked and was given permission to revise and extend his remarks.)

Mr. EDWARDS of California. Mr. Speaker, my colleagues have explained this bill correctly and in detail, and I will not repeat it, but I do want to thank my chairman, the gentleman from Texas [Mr. BROOKS], the gentleman from Michigan [Mr. DINGELL], the gentleman from Massachusetts [Mr. MARKEY] and, of course, our ranking minority member, the gentleman from Illinois [Mr. HYDE], who has been of such enormous help in this difficult bill. It was a difficult bill to write, because it dealt with a subject that makes us all uneasy, which is a constitutional issue having to do with the fourth amendment.

We were determined when we started that we preserve the principle that we established in 1968 in the Omnibus Control and Safe Streets Act, that there must be a warrant by a court before there is any kind of listening in. In addition, we wanted to make sure that all privacy considerations and civil liberties be protected, and that is what we did. We drew the bill very narrowly, and in important instances we tightened existing controls over the police and the FBI. So the result is tougher standards for the FBI and the police in going through any kind of wiretapping.

So I think we did a good job. I guarantee that we protected to the best of our ability the civil liberties of Americans.

The FBI came to us several years ago and said that new technologies were giving them increasing problems carrying out wiretaps.

We said, you have to prove there is a problem before we legislate.

Well, they did their homework, and they proved there is a problem. They have submitted 183 cases, from all over the country, involving many of the new technologies and services.

The industry also has admitted there are technological problems.

So we worked with industry, the FBI, and privacy advocates to develop a bill. Original administration proposals had no privacy provisions and would have given the FBI control over the phone system.

There was a great deal of compromise, and the result is before the House today.

The bill requires common carriers to meet basic functional requirements allowing law enforcement to continue to carry out wiretaps.

The bill allows industry to develop the standards for meeting those requirements.

It provides $500 million over 4 years to pay the costs of modifying existing equipment to comply.

The question of costs was very difficult. The bill before you takes a reasonable middle course. Industry will be required to bear only the reasonable costs of compliance after 4 years. The FCC will determine what is reasonable based on factors specified in the bill.

We dealt with the scope issue very carefully. We cover common carriers, including competitive access providers and companies such as teleport.

We have worked with the gentleman from Virginia, [Mr. BOUCHER] on the question of cost, and he has substantially improved the bill. The contributions made by the Energy and Commerce Committee have been tremendously helpful.

The bill improves privacy protection. We raise the standard for access to transactional records, and require a court order. We improve the protections for cordless phones and cellular phones. We place limits on the ability of law enforcement to use portable phones as tracking devices.

In summary, Mr. Speaker, I urge approval of this bill.

Mr. HYDE. Mr. Speaker, before I yield to the gentleman from Ohio, I want to again congratulate the gentleman from California [Mr. EDWARDS] the distinguished chairman of the Subcommittee on Civil and Constitutional Rights. No one is more sensitive to the fragility of civil liberties and civil rights than he. This bill would not have passed without his attention and care and concern, and I think the country owes him a debt of gratitude for his work in this and so many other things.

Mr. Speaker, I am pleased to yield 3 minutes to the distinguished gentleman from Ohio [Mr. OXLEY].

(Mr. OXLEY asked and was given permission to revise and extend his remarks.)

Mr. OXLEY. Mr. Speaker, I rise in strong support of the Digital Telephony Act of 1994. As mentioned, the purpose of this bill is to safeguard the ability of law enforcement agencies to carry out court-ordered wiretaps.

As a former FBI special agent, I know that the court-authorized interception of communications is one of our most important tools in the investigation of criminal conduct. By necessity, wiretaps are relied upon in the investigation of drug kingpins, terrorists, and others who would use telecommunications networks to further their criminal ends.

Currently, the telecommunications industry is undertaking revolutionary changes in its technology, changes that could make it impossible for police agencies to execute lawful court orders. In some instances, cellular technology and new digital features have already frustrated court-ordered wiretaps.

I want to emphasize that this measure would not expand the authority of law enforcement in any way. It would merely ensure that it remains technically feasible to access communications. Those who suggest that this legislation gives Government new power to pry into people's lives are simply mistaken.

One area of controversy that arose during consideration of the bill concerned the issue of cost—specifically, how great the expense of implementation will be and who should bear it. I want to state my satisfaction with the compromise that has been reached, but also express my willingness to revisit the issue if necessary. In the meantime, I have asked the Office of Technology Assessment to provide an analysis of the cost of implementing the bill.

I wish to take this opportunity to commend FBI Director Freeh, his able staff, and the Committee on the Judiciary for their work on this legislation. I also would like to thank Chairman DINGELL, Chairman MARKEY, Congressman MOORHEAD and Congressman FIELDS for their contributions, along with the gentleman from California [Mr. EDWARDS] and the gentleman from Texas [Mr. BROOKS].

□ 2050

Mr. Speaker, I specifically want to point out how hard the new FBI Director Freeh worked on this particular legislation. Had it not been for him, we would not be here tonight on the suspension calendar.

Mr. Speaker, the need for legislative action is clear. Without it, U.S. authorities will be unequipped to protect the Nation from organized crime, terrorism, drug trafficking, espionage, and other threats.

Mr. Speaker, I urge all Members to support this vital legislation.

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, Oct. 4, 1994.

Hon. MICHAEL G. OXLEY,
U.S. House of Representatives
Washington, DC.

DEAR CONGRESSMAN OXLEY: I am writing to request your support for enactment of the "Communications Assistance for Law Enforcement Act," H.R. 4922. It is scheduled to be voted upon today under suspension of the rules.

This legislation is of extreme importance to all federal, state, and local law enforcement agencies. The bill has the full support of every major law enforcement organization in the country as well as the entire intelligence community.

If enacted, this legislation will prevent new telecommunications technologies from continuing to impede law enforcement agencies' lawful conduct of court-ordered electronic surveillance, without in any way diminishing the privacy of our citizens or hampering the deployment of new telecommunications technology. Indeed, the legislation contains numerous new privacy-enhancing provisions. Passage of this legislation is extremely critical, since without it effective law enforcement, the public safety, and national security will be put at unacceptable risk. Failure to enact it will rob law enforcement officers of a critical tool they use to fight terrorism, drug-trafficking cartels, organized and violent crime, and other life-threatening felonies.

This legislation is the product of an intense and diligent effort by the Senate and House Judiciary Committees, as well as the House Energy and Commerce Committee, to achieve a delicate balance of law enforcement, privacy, and telephone industry interests and concerns. It is sponsored on the House side by Congressmen Edwards and Hyde. This legislation is a remarkable achievement because of its balanced, fair, and equitable treatment of all affected parties, both with regard to responsibilities and cost allocation.

Every day that passes without this essential legislation means that law enforcement will be increasingly stripped of a great weapon against crime and a vital shield to protect the public. Just last week a wiretap in a terrorism investigation was stymied because of digital technology. Similarly, every day that passes means that the cost of solving the problem will grow ever greater. I can't emphasize too strongly that enactment of this legislation cannot wait.

I trust that you will appreciate both the extreme significance of this problem, as well as the extreme importance of this well-crafted legislative solution to correct it. On behalf of the entire law enforcement and intelligence communities, I urgently request your help to ensure that we in law enforcement can continue to do our job of effectively protecting the American public against the violent gangsters and terrorists who prey on society through your support for passage of H.R. 4922.

Sincerely yours,

LOUIS J. FREEH,
Director.

Mr. Speaker, I include for the RECORD a letter from Director Freeh.

Mr. BROOKS. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. POSHARD). The question is on the motion offered by the gentleman from Texas [Mr. BROOKS] that the House suspend the rules and pass the bill, H.R. 4922, as amended.

The question was taken.

Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to the provisions of clause 5, rule I, and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

AMENDING ALEUTIAN AND PRIBILOF ISLANDS RESTITUTION ACT

Mr. BROOKS. Mr. Speaker, I move to suspend the rules and pass the Senate bill (S. 1457) to amend the Aleutian and Pribilof Islands Restitution Act to increase authorization for appropriation to compensate Aleut villages for church property lost, damaged, or destroyed during World War II, as amended.

The Clerk read as follows:

S. 1457

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

SECTION 1. INCREASE IN AUTHORIZATIONS.

(a) IN GENERAL.—Section 205(d)(4) of the Aleutian and Pribilof Islands Restitution Act (50 U.S.C. App. 1989c-4(d)(4)) is amended by striking "$1,400,000" and inserting "$4,700,000".

(b) FUND.—If the Fund referred to in section 205(a) of the Aleutian and Pribilof Islands Restitution Act (50 U.S.C. App. 1989c-4(a)) has been terminated pursuant to section 203(d) of such Act (50 U.S.C. App. 1989c-2(d)), upon the appropriation of additional funds pursuant to this Act, the Fund shall be reestablished.

(c) USE OF FUNDS.—The funds appropriated pursuant to this Act shall be used solely for the renovation, replacement, and restoration of Church property lost, damaged, or destroyed during World War II.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas [Mr. BROOKS] will be recognized for 20 minutes, and the gentleman from Pennsylvania [Mr. GEKAS] will be recognized for 20 minutes.

The Chair recognizes the gentleman from Texas [Mr. BROOKS].

Mr. BROOKS. Mr. Speaker, I yield myself such time as I may consume.

(Mr. BROOKS asked and was given permission to revise and extend his remarks.)

Mr. BROOKS. Mr. Speaker, I rise in support of S. 1457, to amend the existing Aleutian and Pribilof Islands Restitution Act to increase—from $1.4 million to $4.7 million—the authorization of appropriation to compensate Aleut villages for church property lost, damaged, or destroyed during World War II.

The increase is based on the 1993 report by the Department of Interior—which was required by the act—providing an estimate for repair and restoration of the property.

I'm pleased that both the Aleutian Church Restoration Society and the Aleutian/Pribilof Islands Association have provided letters that state: "Any increase in authorization under this bill will be spent solely for the restoration/renovation of Orthodox church property lost, damaged or destroyed during the war.

I urge an aye vote for S. 1457.

Mr. Speaker, I reserve the balance of my time.

Mr. GEKAS. Mr. Speaker, I yield myself such time as I may consume.

I, too, strongly support the passage of this legislation. Many Americans are too quick to forget that while we all were disgraced by the internment of the Japanese during World War II, that the Aleutian Indians as well were victims of that grand injustice perpetrated during that time.

If I wanted to speak more eloquently on the question, I would have to turn to the walking encyclopedia of matters Alaskan, to the resident expert, the gentleman from Alaska [Mr. YOUNG].

Mr. Speaker, I yield such time as he may consume to the gentleman from Alaska [Mr. YOUNG].

(Mr. YOUNG of Alaska asked and was given permission to revise and extend his remarks.)

Mr. YOUNG of Alaska. Mr. Speaker, I thank the gentleman from Pennsylvania [Mr. GEKAS] for yielding time to me. I want to thank the gentleman from Texas [Mr. BROOKS] for bring this legislation to the floor.

The Congress has in the past acted on legislation introduced by myself and other Members of this body to give restitution to the members that remain for the internment which occurred. This is one of the better pieces of legislation which we passed, and I suggest respectfully that this is just a follow-up.

Again, the bill amends the Aleutian-Pribilof Restitution Act by increasing the authorization for appropriations to compensate Aleut villages in Alaska for church property damaged and destroyed during World War II. Some of the churches were destroyed in military operations as part of U.S. efforts to recapture Attu and Kiska. Other churches were looted and burned. Keep in mind, Alaska was the only State that was invaded during World War II.

The Aleutian people themselves are the ones that suffered the most during this activity. This bill amends the existing authorization to allow full compensation of the Aleut people for the destruction of their churches. This also is the legislation of my senior Senator, Senator TED STEVENS. I suggest respectfully this is a sort of a tribute to his effort and interest in my constituents and his own constituents.

I urge my colleagues to support the bill.

Mr. BROOKS. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

Mr. GEKAS. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas [Mr. BROOKS] that the House suspend the rules and pass the Senate bill, S. 1457, as amended.

The question was taken.

Mr. WALKER. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

United States Senate

Beryl A. Howell
Counsel

Subcommittee on Technology
and the Law
Committee on the Judiciary

815 Hart Building
Washington, D. C. 20510
(202) 224-3406

file: digital telephony

SECTION-BY-SECTION ANALYSIS FOR H.R. 4922

94 OCT 24 A 8:49

The bill consists of the following three titles:

- o TITLE I consists of twelve sections, which may be cited as the Communications Assistance for Law Enforcement Act" ("CALEA") and deal with law enforcement's wiretap capability and capacity needs.

- o TITLE II amends Title 18 of the United States Code by expanding the privacy protection of the Electronic Communications Privacy Act to cover cordless phones and certain radio-based communications; prohibiting the fraudulent alteration of cellular telephones; requiring a court order for the disclosure of transactional data on electronic communication services; limiting the use of pen registers that intercept information other than dialing or signaling information; and by making other technical changes.

- o TITLE III amends the Communications Act of 1934 by requiring the Federal Communications Commission ("FCC") to prescribe rules for implementing CALEA's systems security and integrity requirements, by authorizing common carriers to petition the FCC to adjust charges to recover costs of compliance with CALEA, and by making clerical and technical amendments and eliminating expired and outdated provisions of the communications laws.

TITLE 1. INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS. This Title contains twelve sections numbered 101 through 112 and defines more precisely the assistance that telecommunications carriers are required to provide in connection with court orders for wire and electronic interceptions, including pen registers and trap and trace devices.

Section 101 names this title the "Communications Assistance for Law Enforcement Act."

Section 102 provides definitions for "call-identifying information," "electronic messaging services," "information services," "government," "telecommunications support services," and "telecommunications carrier."

The term "call-identifying information" means the dialing or signaling information that identifies the origin and destination of a wire or electronic communication generated or received by a subscriber by means of any equipment, facility or service of a telecommunications carrier. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization.

The term "electronic messaging services" means software-based services that enable data, images, sound, writing or other information to be shared among computing devices controlled by the senders or recipients of the messages.

The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United State, and any state or political subdivision thereof authorized by law to conduct electronic surveillance.

The term "information services" means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, but does not include any capability for a telecommunications carrier's internal management, control or operation of its telecommunications network. Included in the definition of information services are electronic publishing, electronic messaging services, and services permitting customers to retrieve from, and file information in, information storage facilities.

The term "telecommunications support services" means a product, software or service used by a telecommunications carrier for the internal signaling or switching of its network. There are currently over one hundred such support service providers that provide common carriers with specialized support services.

A "telecommunications carrier" is defined as any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, and includes a commercial mobile service, as defined in section 332(d) of the Communications Act. This definition encompasses such service providers as local exchange carriers, interexchange carriers, competitive access providers (CAPS), cellular carriers, providers of personal communications services (PCS), satellite-based service providers, cable companies that offer telephony, and any other common carrier that offers wireline or wireless service for hire to the public. It also includes such services as call forwarding, speed dialing and the call forwarding portion of a voice mail service.

"Telecommunications carrier" does not include persons or entities to the extent they are engaged in providing information services, such as electronic mail providers, on-line services providers, such as Compuserve, Prodigy, America On line or Mead Data, or commercial Internet providers.

In addition, for purposes of this Act, the FCC is authorized to deem other persons and entities to be telecommunications carriers subject to the assistance requirements in section 103 to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public and it is in the public interest to deem them a telecommunications carrier for the purposes of CALEA. The FCC is also authorized, after consultation with the Attorney General, to exempt classes or categories of telecommunications carriers.

Section 103, entitled "Assistance capability requirements," consists of four subsections. **Subsection (a)** sets forth four "Capability Requirements," which every telecommunications carrier is required to meet in connection with those services or facilities that allow customers to originate, terminate or direct communications. The first requirement is expeditiously to isolate and enable the government, pursuant to court order or other lawful authorization, to intercept all wire and electronic communications in the carrier's control to or from the equipment, facilities or services of a subscriber, concurrently with the communications' transmission, or at any later time acceptable to the government.

The second requirement is expeditiously to isolate and enable the government, pursuant to court order or other lawful authorization, to access reasonably available call-identifying information about the origin and destination of communications. Access must be provided in such a manner that the information may be associated with the communication to which it pertains and is provided to the government before, during or immediately after the communication's transmission to or from the subscriber, or at any later time acceptable to the government.

Call identifying information obtained by pen register and trap and trace devices may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number. Orders authorizing the use of trap and trace and pen register devices are obtained upon certification to the court that information likely to be obtained is relevant to an ongoing criminal investigation; to obtain location information, a probable cause showing is required.

The third requirement is to make intercepted communications and call identifying information available to government, pursuant to court order or other lawful authorization, so they may be transmitted over lines or facilities leased or procured by law enforcement to a location away from the carrier's premises.

The final requirement is to meet these requirements with a minimum of interference with the subscriber's service and in such a way that protects the privacy of communications and call identifying information that are not targeted by electronic surveillance orders, and that maintains the confidentiality of the government's interceptions.

Subsection (b) limits the scope of the assistance requirements in several important ways. First, law enforcement agencies are not permitted to require the specific design of systems or features, nor prohibit adoption of any system or feature, by wire or electronic communication service providers or equipment manufacturers. The legislation leaves it to industry to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communications session can be intercepted at some point.

Second, the capability requirements only apply to those services or facilities that enable a subscriber to make, receive or direct calls. They do not apply to information services, such as the services of electronic mail providers, on-line services, such as Compuserve, Prodigy, America Online or Mead Data, or the services of Internet access providers. Nor do they apply to private networks or services merely supporting the transport or switching of communications for the sole purpose of interconnecting carriers. Thus, a carrier providing a customer with a service or facility that allows the customer to obtain access to a publicly switched network is responsible for complying with the capability requirements. On the other hand, for communications handled by multiple carriers, a carrier that does not originate or terminate the message, but merely interconnects two other carriers, is not subject to the requirements for the interconnection part of its facilities.

Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. § 2518(4). Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access.

Subsection (c) allows a carrier, in emergency or exigent circumstances, to fulfill its obligation to deliver communications to law enforcement under the third capability requirement by allowing monitoring on the carrier's premises.

Subsection (d), entitled "Mobile Service Assistance Requirement," addresses the responsibility of the providers of commercial mobile service who can no longer deliver a message or call identifying information to law enforcement because the subscriber, the message and the call identifying information have left the provider's service area. In such a case, the provider that had the assistance responsibility is not required to continue providing the government with the content of the communication or call identifying information, but must notify the government which carrier or service provider has subsequently picked up the content or call identifying information and begun serving the subscriber.

Section 104, entitled "Notices of capacity requirements," places the burden on the government to estimate its capacity needs and to do so in a cost-conscious manner, while also providing carriers with a "safe harbor" for capacity. **Subsection (a)** requires the Attorney General, within one year of enactment, after notice and comment, to publish in the Federal Register and provide to appropriate industry associations and standards bodies notices of both the maximum capacity and the actual capacity required to accommodate all intercepts, pen registers, and trap and trace devices the government (including federal, state and local law enforcement) expects to operate simultaneously.

The actual capacity relates to the number of intercepts the government will need to operate upon the date that is four years after enactment. The maximum capacity relates to the greatest number of intercepts a particular system must be capable of implementing simultaneously at some time farther in the future.

The Attorney General is directed to develop the notices after consultation with local and state law enforcement authorities and the carriers, equipment manufacturers and providers of support services. The Attorney General is given flexibility in determining the form of the notice. For example, the notice may be based upon the type of equipment, type of service, number of subscribers, type or size of carrier, nature of the service area, or any other measure. The notice must identify, to the maximum extent practicable, the capacity required at specific geographic locations.

Subsection (b) provides that, subject to the reimbursement conditions in subsection (e) below, telecommunications carriers must ensure that, within three years after publication of the notice, or within four years after enactment, whichever is longer, they have the initial capacity and the maximum capacity to execute all electronic surveillance orders. If the Attorney General publishes the first capacity notices <u>before</u> the statutory time of one year has elapsed, compliance by carriers must be achieved at the same time as the effective date in Section 111(b) of CALEA. In the event the Attorney General publishes the notices <u>after</u> the one year statutory time limit, carriers will have three years thereafter to comply, which time period will fall after the effective date in Section 111(b) of CALEA.

Subsection (c) requires the Attorney General periodically to give telecommunications carriers notice of any necessary increases in maximum capacity. Carriers will have at least three years, and up to any amount of time beyond three years agreed to by the Attorney General, to comply with the increased maximum capacity requirements.

Subsection (d) requires telecommunications carriers, within 180 days of publication of the capacity notices, to submit to the Attorney General a statement identifying any of their systems or services that do not meet the capacity requirements set forth in the notices.

Subsection (e) requires the Attorney General to review the carriers' statements and authorizes the Attorney General, subject to the availability of appropriations, to agree to reimburse a carrier for reasonable costs directly associated with any modifications to attain the capacity requirements. Until the Attorney General agrees to such reimbursement, the carrier shall be considered to be in compliance with the capacity notices.

<u>Section 105</u> protects systems security and integrity by requiring that any electronic surveillance effected within a telecommunications carrier's switching premises be activated only with intervention by an individual officer or employee of the carrier. The switching premises include central offices and mobile telephone switching offices (MTSOs). The officer or employee must act in accordance with regulations prescribed by the FCC.

This makes clear that government agencies do not have the authority to activate remotely interceptions within the premises of a telecommunications carrier. All executions of court orders or authorizations requiring access to the switching facilities will be made <u>through</u> individuals authorized and designated by the telecommunications carrier. Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the telecommunications carrier, depending upon the amount of assistance the government requires.

<u>Section 106</u>, in **subsection (a)**, requires a telecommunications carrier to consult with its own equipment manufacturers and support service providers to identify those services or equipment to which modifications must be made for the carriers to comply with the capability and capacity requirements. **Subsection (b)** requires manufacturers of telecommunications transmission or switching equipment and support services providers to make available to their customers who are telecommunications carriers the necessary modifications on a reasonably timely basis and at a reasonable charge.

These responsibilities of the manufacturers and support services providers make clear that they have a critical role in ensuring that lawful interceptions are not thwarted. Without their assistance, telecommunications carriers likely could not comply with the assistance capability requirements.

Section 107 establishes a mechanism for implementation of the assistance capability requirements that defers, in the first instance, to industry standard-setting organizations. **Subsection (a)** directs the Attorney General, in coordination with other law enforcement agencies, to consult with associations and standard-setting bodies of the telecommunications industry.

Carriers, manufacturers and support service providers will have a "safe harbor" and be considered in compliance with the assistance capability requirements if they comply with publicly available technical requirements or standards designed in good faith to implement the assistance requirements.

This subsection states affirmatively that the absence of publicly available technical requirements or standards will not preclude carriers, manufacturers or support service providers from deploying a technology or service, nor relieve them from their obligations under CALEA. Thus, even absent such requirements or standards, carriers must still comply with the assistance capability requirements, and manufacturers and support services providers still have a duty to assist carriers.

Subsection (b) provides a forum at the FCC in the event a dispute arises over the technical requirements or standards. Anyone can petition the FCC to challenge any technical requirements or standards issued by industry associations or bodies under this section, or, if none exist, to establish such requirements or standards. In taking any action under this section, the FCC is directed to meet the assistance capability requirements by cost-effective methods, protect privacy and security of communications that are not the targets of court-ordered electronic surveillance, minimize the cost of compliance on residential ratepayers, and serve the policy of the United States to encourage the provision of new technologies and services to the public.

If an industry technical requirement or standard is set aside or supplanted by the FCC, the FCC is required to consult with the Attorney General and establish a reasonable time and conditions for compliance with and the transition to any new standard. The FCC may also define the assistance obligations of the telecommunications carriers during this transition period.

Subsection (c) authorizes the FCC to grant telecommunications carriers an additional two years to achieve compliance with the assistance capability requirements beyond the four years provided in Section 111(b) of CALEA. The FCC may grant a petition for relief from compliance with the assistance capability requirements for up to two years in circumstances where the carrier can show that compliance with those requirements is not reasonably achievable through application of technology available within the four year compliance period. The Attorney General will reimburse the carrier for any necessary modifications made during the extension period.

Any extension granted under this subsection applies only to that part of the carrier's business on which the equipment, facility, or service at issue is used.

<u>Section 108</u> provides guidance to the courts for any order issued to enforce the requirement of CALEA. **Subsection (a)** defines the grounds for issuance of an enforcement order. First, the court must find that law enforcement has no alternatives reasonably available for implementing the order through use of other technologies or capabilities, or by serving the order on another carrier or service provider. Essentially, the court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception.

Second, the court must find that compliance with the requirements of CALEA is reasonably achievable through application of available technology, or would have been reasonably achievable if timely action had been taken. Of necessity, a determination of "reasonably achievable" will involve a consideration of economic factors. This limitation is intended to excuse a failure to comply with the assistance capability requirements or capacity notices where the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. This subsection recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of CALEA.

In the event that either of these grounds is not met, the court may not issue an enforcement order and the carrier may proceed with deployment, or with continued offering to the public, of the equipment, facility, or service at issue.

Subsection (b) requires a court upon issuance of an enforcement order to set a reasonable time and conditions for complying with the order. In determining what is reasonable, the court may consider as to each party before it a number of enumerated factors.

Subsection (c) places three limitations on the court's authority to issue enforcement orders. First, an enforcement order may not be issued requiring a carrier to exceed the capacity set forth in the Attorney General's notices under section 104.

Second, an enforcement order may not require a carrier to comply with the assistance capability requirements if the FCC has determined, pursuant to its authority under section 109(b)(1), that such compliance is not reasonably achievable. However, if the Attorney General agrees, pursuant to section 109(b)(2), to pay the incremental costs to make compliance reasonably achievable, this limitation does not pertain.

Finally, an enforcement order may not require a carrier to modify equipment, facilities or services deployed before January 1, 1995, to comply with the assistance capability requirements unless the Attorney General has agreed to pay for all reasonable costs directly associated with the modifications necessary for compliance. However, if such non-compliant equipment, facilities or services are replaced, significantly upgraded or otherwise subject to major modification after January 1, 1995, this limitation does not pertain.

Section 109, entitled "Payment of Costs of Telecommunications Carriers To Comply With Capability Requirements" requires in **subsection (a)** that the Attorney General pay all reasonable costs directly associated with modifications to equipment, facilities and service deployed before January 1, 1995 to ensure compliance with the assistance capability requirements.

Subsection (b) deals with payments of costs for equipment, facilities and services installed or deployed after January 1, 1995. For such equipment, facilities and services, **paragraph (b)(1)** authorizes telecommunications carriers and other interested persons to petition the FCC for a determination of whether compliance with the assistance capability requirements is reasonably achievable. The FCC is given 1 year after the petition is filed to make this determination. In making this determination, the FCC is directed to determine whether compliance would impose significant difficulty or expense on the carrier or users, and to consider a number of enumerated factors, including the effect on public safety and national security, the rates for basic residential telephone service, and the need to protect privacy and security of communications not authorized to be intercepted.

Paragraph (b)(2) provides that if compliance with the assistance capability requirements is not reasonably achievable for equipment, features or services deployed after January 1, 1995, the Attorney General is authorized, on application by a carrier, to agree to pay additional reasonable costs to make compliance reasonably achievable. Absent such agreement, the carrier will be deemed to be in compliance.

Subsection (c) directs the Attorney General to allocate appropriated funds to carry out the purposes of CALEA in accordance with law enforcement's priorities.

Subsection (d) provides that if a telecommunications carrier requests payment for modifications to equipment, facilities or services deployed on or before January 1, 1995 to achieve compliance with the assistance capability requirements, and the Attorney General does not agree to pay, the equipment, feature or service in question will considered to be in compliance, until it is replaced, significantly upgraded or otherwise undergoes major modification.

Subsection (e) authorizes the Attorney General, after notice and comment, to establish regulations to effectuate the timely and cost-efficient processing of any payment by the government to carriers under CALEA, under chapters 119 and 120 of title 18, United States Code, and under the Foreign Intelligence Surveillance Act of 1978. The Attorney General is further directed to consult with the FCC about issuing regulations to determine reasonable costs under CALEA. Such regulations must minimize the cost to the Federal government and maintain the confidentiality of trade secrets, while permitting recovery from the government of (i) the direct research and development costs that have not been recovered from any other governmental or nongovernmental entity, (ii) the direct costs attributable to compliance with CALEA of personnel training and the deployment or installation of equipment or facilities, and (iii) in the case of modifications that may be used for purposes other than for lawfully authorized electronic surveillance, only the incremental costs attributable to compliance with CALEA. Such regulations will require telecommunications carriers to submit to the Attorney General claims for payment and such information as the Attorney General may require.

<u>Section 110</u> authorizes $500,000,000 to be appropriated for fiscal years 1995 through 1998, which encompass the four years after enactment, to carry out the purposes of CALEA. Such sums are authorized to remain available until expended.

<u>Section 111</u> sets the effective date for compliance with the assistance capability requirements in section 103 and the systems security and integrity requirement in section 105 as four years after enactment. All other provisions take effect upon date of enactment.

Section 112 requires the Attorney General, beginning in 1995, to report annually to Congress on or before November 30, on the monies expended under CALEA. This report must include detailed accountings of the amounts paid, and expected to be paid, to each carrier and identify the equipment, facility or service for which such payments were, or are going to be, made.

In addition, the General Accounting Office ("GAO") is required to report on or before April 1, 1996 and every two years thereafter, on the costs of compliance with CALEA, including costs incurred, and projected to be incurred, by the Attorney General and telecommunications carriers. In addition, GAO's report must include a description of the equipment, facilities or services for which costs have been or are expected to be incurred.

TITLE II. AMENDMENTS TO TITLE 18, UNITED STATES CODE. This title contains eight amendments to the criminal code in title 18 of the United States Code.

Section 201 adds to title 18 a new section 2522, entitled "Enforcement of the Communications Assistance for Law Enforcement Act." New section 2522(a) provides that a court may order telecommunications carriers, equipment manufacturers and support service providers to comply forthwith with the requirements of CALEA in circumstances where an electronic surveillance order or authorization has been issued but cannot be effected because a carrier has failed to comply with those requirements. An order under this subsection must be issued in accordance with the grounds for issuance and limitations in section 108 of CALEA.

New section 2522(b) authorizes the Attorney General, in the absence of a particular electronic surveillance order or authorization, to apply in a civil action to an appropriate United States Court for an enforcement order directing a telecommunications carrier, equipment manufacturer and support services provider to comply with CALEA. In order to avoid disparate enforcement actions throughout the country which could be burdensome for telecommunications carriers, this authority is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.

New section 2522(c) authorizes a court to impose upon any carrier, equipment manufacturer or support service provider a civil penalty up to $10,000 per day for each day in violation after issuance of the order or at such later time as the court may order. In setting the appropriate amount of the fine, a court may consider a number of enumerated factors, including the nature, circumstances, and extent of the violation, and, with respect to the violator, ability to pay, good faith efforts to comply in a timely manner, effect on ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require.

New section 2522(d) makes clear that the definitions under this section are the same as in section 102 of CALEA.

Subsection (b) sets forth three conforming amendments to title 18. First, a new sentence is added to 18 U.S.C. § 2518(4) to make clear that an order may be issued under new section 2522 to enforce the assistance capability and capacity requirements of CALEA. This makes clear that court orders under CALEA are intended to compliment the existing requirement in section 2518(4) that orders authorizing electronic surveillance may direct providers of wire or electronic communications services or any "other person ...[to] furnish ... forthwith all information, facilities, and technical assistance necessary to accomplish the interception."

Second, a new subsection is added to section 3124 of title 18, which authorizes orders for pen registers and trap and trace devices, to make clear that an order may be issued under new section 2522 to enforce the assistance capability and capacity requirements of CALEA.

Finally, the table of sections at the beginning of chapter 119 of title 18 is amended by adding a reference to new section 2522.

Section 202 extends privacy protection to cordless telephones. The Electronic Communications Privacy Act (ECPA), which amended the wiretap statute in 1986, exempted from the protection of the Act "the radio portion of a cordless telephone that is transmitted between the cordless telephone handset and the base unit." 18 U.S.C. § 2510(1) & (12). In view of the current ubiquitous use of such phones and the public expectation that such calls are protected just like cellular telephone calls, a 1991 Privacy and Technology Task Force ("Task Force") organized by Senator Patrick J. Leahy (D-VT) recommended that privacy protection be extended to the radio portion of communications transmitted between the handset and base unit of cordless telephones.

Consistent with the Task Force's recommendations and legislation proposed by the Clinton Administration, the bill would delete the exceptions for cordless phones and impose the same penalties applicable to the unauthorized interception of the radio portions of cellular telephones. Specifically, for first offenders, who intentionally intercept the radio portions of cordless phone, but not for an enumerated bad purpose, the penalty is a $500 criminal fine. If the interception is for a tortious or illegal purpose or for direct or indirect commercial advantage or private financial gain, the offense is punishable as a one-year misdemeanor with fines of up to $100,000 under 18 U.S.C. § 3623.

Section 203, entitled "Radio-based Data Communications," expands privacy protection to electronic communications transmitted by radio. ECPA does not protect communications that are "readily accessible to the general public," which includes radio communications, unless they fit into one of five specified categories. These excepted categories enjoy protection because they usually are not susceptible to interception by the general public.

The bill would add "electronic communication" as a category of radio communication covered by the wiretap statute. This would provide protection for electronic data communications, even when such communications may be transmitted by radio.

Section 204 amends the penalty provision in 18 U.S.C. § 2511(4)(b) to treat communications using modulation techniques with nonpublic parameters in the same fashion as those where encryption has been employed to secure communications privacy. This paragraph refers to spread spectrum radio communications, which usually involve the transmission of a signal on different frequencies where the receiving station must possess the necessary algorithm in order to reassemble the signal.

Section 205 makes a technical correction to 18 U.S.C. § 2511(2)(a)(i), which currently permits interception of <u>wire</u> communications by a wire or electronic service provider in the normal course of business to render services or protect rights or property. The bill would expand the exception to include <u>electronic</u> communications.

Section 206, entitled "Fraudulent Alteration of Commercial Mobile Radio Instruments," amends the Counterfeit Access Device law to criminalize the use of cellular phones that are altered, or "cloned," to allow free riding on the cellular phone system. Specifically, this section prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to obtain unauthorized access to telecommunications services. A scanning receiver is defined as a device used to intercept illegally wire, oral or electronic communications. The penalty for violating this new section is imprisonment for up to fifteen years and a fine of the greater of $50,000 or twice the value obtained by the offense.

Section 207 increases privacy protection for transactional information. Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, **subsection (a)** eliminates the use of a subpoena by law enforcement to obtain from a provider of electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, law enforcement must show facts which establish why such records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, address, telephone billing toll record, telephone or other subscriber number or identity, length of service, and the types of services the subscriber or customer utilized.

Subsection (b) requires government agencies installing and using pen register devices to use, when reasonably available, technology that restricts the information captured by such devices to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialled digits that would otherwise be captured.

Section 208 authorizes Acting Deputy Attorneys General in the Criminal Division of the Department of Justice to approve applications under 18 U.S.C. § 2516(1) to a Federal judge for an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation or other Federal agencies.

TITLE III. AMENDMENTS TO THE COMMUNICATIONS ACT OF 1934.
This Title contains four sections numbered 301 through 304.

Section 301 adds to the Communications Act of 1934 a new section 229, entitled "Communications Assistance for Law Enforcement Act Compliance," which directs the FCC to issue rules necessary to implement CALEA. In order to implement the systems security and integrity requirement in section 105 of CALEA, such rules must require common carriers to establish policies and procedures so that their officers and employees require the proper authorization to activate interceptions, prevent such interceptions without the proper authorization, and maintain secure and accurate records of both authorized and unauthorized interceptions. The FCC must review carriers' policies and rules regarding compliance with CALEA, and order changes made to ensure compliance. This section also authorizes penalties for a carrier's violation of these rules.

This section allows carriers to petition the FCC to adjust charges and regulations to recover costs expended for equipment and service modifications necessary under CALEA. The FCC may grant these petitions if the costs are reasonable and in the public interest. Finally, the FCC must convene a joint Federal-State board to recommend changes to the FCC's rules with respect to the recovery of costs.

Section 302 amends the schedule of application fees under the Communications Act to charge carriers a $5000 fee for a proceeding under section 109(b) of CALEA.

Section 303 makes clerical and technical amendments to the Communications Act of 1934, the Communications Satellite Act of 1962, the Children's Television Act of 1990, the Telecommunications Authorization Act of 1992, and the Omnibus Budget Reconciliation Act of 1981.

Section 304 eliminates expired and outdated provisions in the Communications Act of 1934 and the Communications Satellite Act of 1962.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

file
digital telephony

94 SEP 19 P2:11

September 17, 1994

MEMORANDUM FOR JAMIE GORELICK
LOUIS FREEH

FROM: Christopher Edley, Jr. CXE

SUBJECT: Funding for Digital Telephony

I am increasingly worried about funding provisions in the digital telephony legislation currently under consideration by Congress. Specifically, I am concerned that the funding source/mechanism for common carrier reimbursement in the bill is virtually unworkable in light of the budget problems you face and the magnitude of the law enforcement needs, as I understand them.

Funding for digital telephony does not appear to be specifically authorized in the Violent Crime Reduction Trust Fund but is permissible under Justice and FBI's generic authorities in the bill (See Title XIX, sec. 190001(b-c)). Coupled with tight discretionary budget constraints facing us, it would be increasingly difficult to secure the necessary discretionary funding to support implementation of the legislation. In light of this, I would expect that Justice's FY 1996 budget request to OMB, or at least outyear plans, would include -- <u>within its ceiling (including the Violent Crime Reduction Trust Fund)</u> -- seed monies for digital telephony. Please inform me if I am mistaken.

As a possible alternative, we have already suggested to you that the bill be amended to put at least some of the reimbursement scheme on the mandatory side of the budget, with offsets provided by increasing fines, penalties or fees within the jurisdiction of the Judiciary Committees. I am told that Hill staff have rejected this idea, as floated by FBI legislative affairs staff. I believe their objections are astoundingly parochial and short-sighted. (Of course, that's not inconsistent with being definitive.) The discretionary caps simply will not accommodate the level of funding contemplated by the FBI and proponents of the reimbursement scheme. That is the harsh reality, from our perspective. It ill-serves the law enforcement cause to pretend that, somehow, the CJS Appropriations subcommittees will discover hundreds of millions of dollars in outlays to handle this new initiative. If you are, as you should be, squeezing the telephony reimbursement program into your outyear planning ceilings, you fully appreciate the problem. I seriously doubt that the President, Vice President or appropriators will cut Census, NIST, or Peacekeeping to make you whole.

So, what are we to do? Let me reiterate OMB's strong support for the Department's efforts in achieving passage of this important legislation. I fear that our failure, thus far, to secure realistic funding provisions will make the ultimate product unworkable.

We look forward to working with you on this problem through the budget season. More immediately, however, feel free to contact me or my staff if, in any way, we can be of assistance to the Department in its search for legislative solutions.

cc: Alice Rivlin
John Podesta
Sally Katzen
Steve Colgate, Assistant Attorney General for Budget

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director — Washington, D.C. 20535

94 SEP 19 P5:01

September 19, 1994

MEMORANDUM FOR: Christopher Edley, Jr.

FROM: Louis J. Freeh, Director, FBI

SUBJECT: FUNDING FOR DIGITAL TELEPHONY

I am shocked at your memorandum dated September 17, 1994. Moreover, on an issue of such importance, I would expect to receive a telephone call, not a memorandum faxed on a Saturday.

For the better part of a year, on behalf of law enforcement and the intelligence community **and with the Administration's full support**, the FBI and I have pursued passage of the digital telephony legislation -- the single most important piece of legislation related to public safety, effective law enforcement, and national security. My direct conversations with Vice President Gore and former OMB Director Panetta underscored their recognition of this matter's importance and the Administration's resolve to safeguard our Nation through passage of, and funding for, this legislation. I am amazed you seem unaware of the Administration's unequivocal substantive and fiscal commitment to this legislation.

For approximately six months, OMB has known that the Senate and House Judiciary Committees would not fund the $500 million authorized in the digital telephony legislation out of the Violent Crime Reduction Trust Fund. The Administration's legislation envisioned that, absent funding from the Trust Fund, funding would be authorized "from the General Fund of the Treasury." Further, OMB recognized that advanced telephony threats were shared by many agencies and that the beneficiaries of the proposed legislation included, among others, the following departments and agencies: Justice; Treasury; Defense; State; CIA; NSA; and, DIA. Thus, your suggestion that the FBI or

Department of Justice "squeez[e] the telephony reimbursement program into ... outyear planning ceilings..." is utterly preposterous and marks a radical departure from the Administration's consistent position.

The FBI and I have worked hard to ensure that this legislation is enacted this session of Congress. With passage imminent, I am appalled that you would jeopardize our efforts and embarrass the Administration through this last minute fiscal flip-flop. In response to numerous congressional inquiries, I have given assurances that "the Administration was good for its word" on funding. Your outrageous memorandum undermines the integrity of **my** word and this effort, including the efforts of countless law enforcement officials -- at all levels of government -- who personally and publicly have supported the legislation.

As you note, OMB strongly supports "efforts in achieving passage of this important legislation." We must avoid, at all costs, counterproductive comments such as those in your memorandum which endanger passage of this critical legislation. I expect the Administration to abide by its commitment made several months ago to obtain funding from the General Fund of the Treasury for the digital telephony initiative, in light of the fact that funding is not available from the Violent Crime Reduction Trust Fund. As you know, that commitment was evident from the Administration's proposal, which had been approved by OMB.

1 - Honorable Bill Clinton
The President
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

1 - Honorable Albert Gore
The Vice President
Old Executive Office Building
Washington, D.C. 20501

1 - Honorable Leon E. Panetta
Chief of Staff
1600 Pennsylvania Avenue, N.W.
Washington, D. C. 20500

1 - Honorable Anthony Lake
Assistant to the President
for National Security Affairs
The White House
Washington, D. C. 20500

1 - Honorable John D. Podesta
Assistant to the President
and Staff Secretary
The White House
Washington, D.C. 20500

1 - Honorable Alice Rivlin
Director-Designate, OMB
Old Executive Office Building
17th St. & Pennsylvania Avenue, N.W.
Washington, D.C. 20503

1 - The Attorney General

1 - The Deputy Attorney General

1 - Assistant Attorney General for Administration
Stephen R. Colgate

ATIS
Alliance for Telecommunications Industry Solutions
Formerly the Exchange Carriers Standards Association
Problem Solvers to the Telecommunications Industry

1200 G Street NW
Suite 500
Washington DC 20005

202-628-6380
Fax: 202-393-5453

COMMITTEES

T1 Committee T-1 Telecommunications
CLC Carrier Liaison Committee
•Network Operations Forum
•Ordering & Billing Forum
•Industry Carriers Compatibility Forum
TCIF Telecommunications Industry Forum
IILC Information Industry Liaison Committee
PEG Protection Engineers Group
05 Standards Committee 05
ECSPC Electronic Communications Service Provider Committee
NRSC Network Reliability Steering Committee

File
Digital Telephony

94 APR 15 P 1 : 56

April 14, 1994

The Honorable Louis J. Freeh
Director, Federal Bureau of Investigation
J. Edgar Hoover FBI Building
Tenth St. and Pennsylvania Ave.
Washington, DC 20535

Dear Director Freeh:

This letter is in reference to the request made during your meeting with telecommunications industry representatives on March 11, 1994, held to discuss industry views regarding the proposed legislation entitled "Digital Telephony and Communications Privacy Improvement Act of 1994". This request reflected a need to identify what technologies/services should be included for compliance in a given time frame. The Electronic Communications Service Provider (ECSP) Committee has not addressed those issues.

The ECSP Committee has investigated certain technologies/services, and has established a prioritized list for managing our study efforts. The Committee has agreed to share this information with you, with the understanding that it is clearly represented as a schedule of work activities. (See attached "Scenario Prioritization Action Team Report.") The report also characterized the nature of the technologies as existing, newly deployed, or emerging. It is important to understand that the purpose of this document was not to establish time schedules for implementation of surveillance capabilities for the technologies/services covered.

We believe the ECSP Committee work already undertaken can be of assistance. We will continue the joint law enforcement and industry approach to identify the technical and operational issues, and find resolution to them.

Sincerely,

K R Raymond | David Worthley

Ken Raymond, NYNEX	David Worthley, FBI
ECSP Committee Co-chair	ECSP Committee Co-chair

Attachments

Alliance for Telecommunications Industry Solutions

cc: The Honorable John D. Podesta
Assistant to the President and Staff Secretary
Ground Floor, West Wing
The White House
Washington, DC 20500

Dr. Michael Nelson
Technology Division
Office of Science and Technology Policy
OEOB, Room 423
Washington, DC 20500

ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS (ECSP)

SCENARIO PRIORITIZATION ACTION TEAM

10-27-93

A. GENERAL

The primary mission of Federal, State and Local law enforcement agencies is to uphold the laws of their respective jurisdictions through investigations of criminal violations. When traditional investigative techniques are exhausted, law enforcement can conduct court ordered electronic surveillance of public telecommunications. This extraordinary technique, which is authorized and monitored by the courts, is critical to law enforcement's mission.

B. CHARTER

Recognizing the numerous combinations of physical, information and service feature scenarios encountered in public telecommunications networks, the ECSP reactivated the Scenario Prioritization Action Team to review the previous priority list of September, 1992, and revise it to reflect current views of existing, newly deployed and emerging technologies.

The team was also charged to refine the work of Charter Area I and document an ongoing process for introducing and prioritizing new technologies and issues into the pipeline for developing recommendations for conducting court-ordered surveillance.

C. PRIORITIES (ATTACHMENT 1)

Upon review of the previous priority list of September, 1992, it was agreed that a format, which lists the various scenario characterizations with technology descriptions indicating the extent of deployment in the public telecommunications network, would be of more value to the ECSP than the previous format.

It was also agreed that, based primarily on law enforcement's needs, three priority groupings would be used to help determine the urgency of need since it was most difficult to ascertain priorities within a particular grouping. No distinction within the priority groupings is intended.

Since resources within ECSP and its constituents are limited, these priorities will help to determine the order of investigation into existing, new and emerging technologies.

D. ECSP PROCESS FOR THE INTRODUCTION AND PRIORITIZATION OF NEW TECHNOLOGIES AND INTERCEPT ISSUES IN TELECOMMUNICATIONS (ATTACHMENT 2)

Industry and Law Enforcement Members and Participants of the ECSP Committee provide inputs regarding new technology and Law Enforcement issues to the plenary of the ECSP Committee.

The Committee considers the inputs and selects those technologies which appear most relevant to Law Enforcement's needs at that time. The ECSP Committee requests the Prioritization and Technology Review (PT&R) Action Team to review one or more selected technologies to determine their impact on intercept capabilities and to recommend any need for a new Action Team or any prioritization of such technologies for ECSP study and resolution. The Committee will also consider all inputs from its members and participants to judge whether its work issues require reprioritization and could ask the PT&R Action Team for a recommendation.

The ECSP Committee receives the recommendations of the PT&R Action Team and decides if there is a need for a new Action Team. Should such be the case, it designates a technology-specific action team to analyze the various possible ways to provide intercept taking into account the several avenues available including the following:

1. Operational/procedural changes which exploit existing capability at very low incremental cost.
2. The development of specialized capability to suit the needs of Law Enforcement by modification of presently deployed or available equipment or software or the addition of supplementary equipment or software for the premises of the service provider or in some cases for the premises of law enforcement agencies.
3. Establishment of the need for a new or modified public standard that would support the need for intercept capability. In this case, entities are identified to pursue the advocates of such a standards development.

These solutions are not mutually exclusive and may even apply in different time frames.

SCENARIO PRIORITY LIST

A/O OCTOBER 27, 1993

PRIORITY 1 (TYPE TECHNOLOGY)

Switch-based solutions in traditional central offices for various services:

- Call forwarding (existing)
- Speed dialing (existing)
- Three-way calling (existing)
- Calling line identification (existing)
- Voice recognition calling (emerging)
- Voice recognition validation (emerging)
- Integrated Services Digital Network (ISDN) - BRI (newly deployed)
- Integrated Services Digital Network (ISDN) - PRI (newly deployed)
- Other CLASS services (newly deployed)

Advanced Intelligent Network (AIN) solutions in Service Management Systems (SMS) and central offices for AIN-type services:

- Call forwarding (newly deployed)
- Calling line delivery (newly deployed)
- Calling name delivery (newly deployed)

Wireless Cellular solutions in Mobile Telephone Switching Offices (MTSO) for cellular-type services:

- Call setup and call content (existing)
- Port capacities (newly deployed)
- Intra-system roaming (existing)
- Inter-system roaming (existing)
- Cellular seamless roaming per IS-41 (emerging)

Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) solutions on physical copper wire facilities (newly deployed):

- BRI Regenerator approach completed March, 1993
- BRI Bridging approach

Personal Communications Services (PCS) (emerging).

SCENARIO PRIORITY LIST (CONT'D.)

A/O OCTOBER 27, 1993

PRIORITY 2 (TYPE TECHNOLOGY)

- Personal Communications Services (PCS) - Satellite services. (emerging)
- Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) solutions on physical copper and fiber facilities. (newly deployed)
- Private Virtual Network (PVN) solutions in central office switches. (newly deployed)
- Voice-mail - switch adjunct. (existing)
- E-mail. (existing)
- Voice dialing/recognition, non-switch based. (emerging)
- Facsimile mail. (newly deployed)

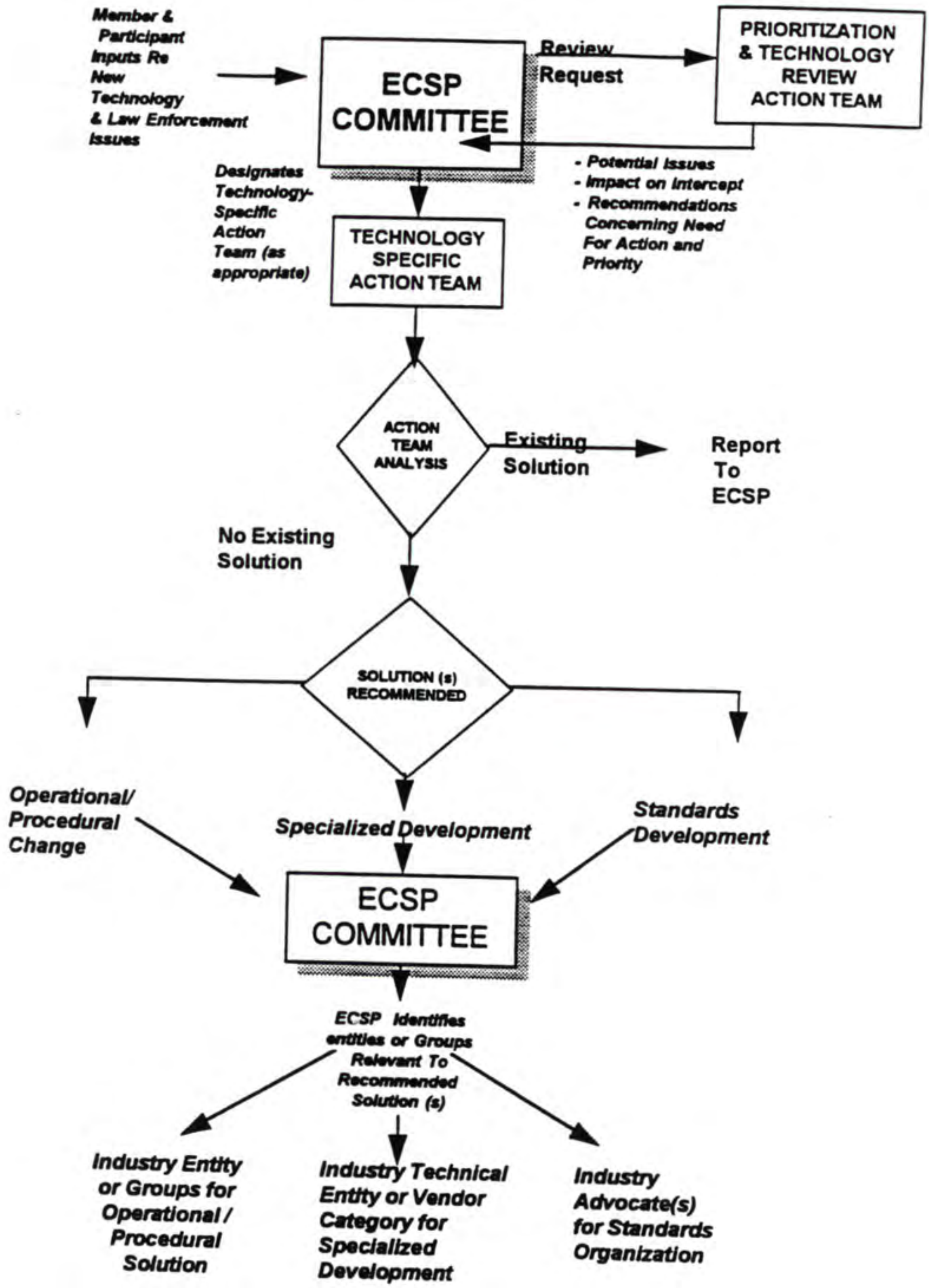
SCENARIO PRIORITY LIST (CONT'D.)

A/O OCTOBER 27, 1993

PRIORITY 3 (TYPE TECHNOLOGY)

- Broadband Integrated Services Digital Network (BISDN) solutions in serving central office switches. (emerging)
- Switched Multi-megabit Digital Services (SMDS) solutions. (emerging)
- High Bit Rate Digital Subscriber Lines (HDSL) solutions. (newly deployed)
- Asymmetrical Digital Subscriber Line (ADSL) solutions. (emerging)
- Intelligent Network (IN) solutions in Service Management Systems (SMS) and central offices for IN services:
  (1) Capability Set 1 (emerging)
  (2) Capability Set 2 (emerging)
- Intelligent Customer Premises Equipment (CPE) interactions with the serving central office switch, e.g., screen based telephony. (emerging)
- Universal personal telecommunications (UPT) services. (emerging)
- Telephone services on coaxial cable. (emerging)

New Technologies & Priority Review Process



DIGITAL PRIVACY AND SECURITY WORKING GROUP

1001 G Street, NW
Suite 950 East
Washington, DC 20001

Jerry Berman 202/347-5400
Leah Gurowitz 202/393-1010

file
DIGITAL telephony

94 MAR 9 A9:34

March 9, 1994

The President William J. Clinton
The White House
Washington, D.C. 20500

The Vice President of the United States
United States Senate
Washington, D.C. 20510

Dear Mr. President and Mr. Vice President:

Telecommunications carriers and other members of the Digital Privacy and Security Working Group are keenly aware of the concerns raised by the Administration regarding the ability to intercept communications transmitted over advanced communications networks.

We are concerned, however, about the nature of the process upon which the Administration has embarked to address these issues. Seeking immediate industry reaction to the FBI's draft legislation and congressional passage of such legislation shortly thereafter is troubling. It suggests curtailment of public debate and of congressional deliberation. Given the interest of the public in these matters and their complexity, it is essential that there be a full public debate on these issues.

Industry is currently cooperating with appropriate authorities to avoid future problems and to expand existing capacities. This is not to say that there have not been some transitional concerns particularly upon the introduction of new technologies that have grown greatly in popularity. But, whenever transitional problems have arisen, industry representatives have worked with law enforcement officials to resolve them.

The FBI's actions are especially troubling in light of our view that legislation is not needed to accomplish the agency's goals. We still see no evidence that current law enforcement efforts are being jeopardized by new technologies. Nor are we convinced that future law enforcement activities will be jeopardized given industry cooperation.

We still believe that continued cooperation by government and industry within the working relationship that has emerged from the 1992 Quantico Joint Government Industry Group will resolve "the digital telephony problem" and preserve the government's current authorities. The discussions have succeeded in identifying specific problems and have begun the process of generating concrete, cost-effective solutions. This process has facilitated a more robust exchange of technical information and an identification of possible new equipment and police tactics needed to achieve law enforcement goals. Nevertheless, we are prepared to work with the Congress and the Administration to attempt to resolve the legitimate concerns of law enforcement.

The signatories to this letter cannot overemphasize how critical it is that any new initiatives in this area preserve the public's confidence in the privacy of information carried over the public switched network. Less than a decade after enactment of the Electronic Communications Privacy Act of 1986, the nation can ill afford to undercut customer privacy expectations. Indeed, on the eve of the National Information Infrastructure's deployment, preserving customer confidence is all the more important. Privacy protection is not a secondary interest here. Survey after survey performed by Professor Alan Westin and others have demonstrated the public's concern with privacy and the security of their communications. We all must seek to maximize those interests and assure the public that their communications are protected.

Sincerely yours,

Apple Computer, Inc.
AT&T
American Civil Liberties Union
Business Software Alliance
Cellular Telecommunications Industry Association
Computer Business Equipment & Manufacturers Assn
Digital Equipment Corporation
Electronic Frontier Foundation
Electronic Messaging Association
GTE Corporation
Information Industry Association
Information Technology Association of America
Iris Associates, Inc.
McCaw Cellular
MCI Communications Corporation
People for the American Way
Software Publishers Association
Sun Microsystems Federal, Inc.
Trusted Information Systems
United States Telephone Association

cc: Louis Freeh, Director, Federal Bureau of Investigation
John Podesta, Office of the President
Michael Nelson, Office of the Vice President
Senator Patrick Leahy
Senator Ernest Hollings
Representitive Don Edwards
Representative Edward Markey

103rd Congress
2nd Session

DRAFT

2/9/94

file DIGITAL Telephony

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 continued law enforcement electronic surveillance access to the content of wire and electronic communications and call setup information when authorized by law, to improve communications privacy protection, and for other purposes.

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

SEC. 1. SHORT TITLE.

This Act may be cited as the "Digital Telephony and Communications Privacy Improvement Act of 1994."

SEC. 2. PURPOSE. The purpose of this Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under chapters 119 and 206 of title 18 and chapter 36 of title 50. Otherwise, except for the provisions in section 4, nothing in this Act is intended to alter any provision contained in the Federal electronic surveillance, pen register, or trap and trace statutes, or those of any state or other jurisdiction. In particular, nothing herein is intended to enlarge or reduce the government's authority to lawfully intercept the content of communications or install or use pen register or trap and trace devices, or to increase or decrease any criminal penalties for unlawfully intercepting the content of communications or installing or using pen register or trap and trace devices, or to alter the provisions regarding service provider assistance, payment for assistance, causes of action, civil liability, or good faith defenses.

The Act is further intended to improve communications privacy protection for cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

SEC. 3. COMMON CARRIER ASSISTANCE.

(a) **<u>New section</u>**. Chapter 109 of title 18, United States Code, is amended by adding the following new section:

"Sec. 2237. Common carrier assistance to government agencies.

"**(a) Assistance requirements.** Common carriers shall be required to provide forthwith, pursuant to court order or lawful authorization, the following capabilities and capacities in order to permit the government to conduct electronic surveillance and pen register and trap and trace investigations effectively:

"(1) The ability to execute expeditiously and simultaneously within a common carrier's system all court orders and lawful authorizations for the interception of wire and electronic communications and the acquisition of call setup information related to the facilities or services of subscribers of such common carrier;

"(2) the ability to intercept the content of communications and acquire call setup information concurrent with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or lawful authorization, to the exclusion of any wire or electronic communication or call setup information of any other subscriber, notwithstanding the mobile nature of the facility or service that is the subject of the court order or lawful authorization or the use by the subscriber who is the subject of the court order or lawful authorization of any features offered by the common carrier;

"(3) the ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service; and

"(4) the ability to receive, in a generally available format, the intercepted content of communications and acquired call setup information at a location identified by the government distant from the facility that is the subject of the interception, from the interception access point, and from the premises of the common carrier (except where emergency or exigent circumstances such as those described in 18 U.S.C. 2518(7), 2518 (11)(b), or 3125, or in 50 U.S.C. 1805(e), necessitate monitoring at the common carrier's premises).

"**(b) Systems security.** The government shall notify a common carrier of any interception of wire or electronic communications or any acquisition of call setup information that is to be effected within the premises of such common carrier pursuant to court order or lawful authorization. After notification, such common carrier shall designate an individual or individuals to activate such interception or acquisition forthwith. Such individual(s) shall be available at all times to activate such interceptions or acquisitions. Such interceptions or acquisitions effected within the premises of a common carrier may be activated only by the affirmative intervention of such individual(s) designated by such common carrier.

"**(c) Compliance date.** To the extent that common carriers providing service within the United States currently cannot fulfil the requirements set forth in subsection (a) of this section, they shall fulfil such requirements within three years from the date of enactment of this Act.

"**(d) Cooperation of support service providers and equipment manufacturers.** Common carriers shall consult, as necessary, in a timely fashion with appropriate providers of common carrier support services and telecommunications equipment manufacturers for the purpose of identifying any services or equipment, including hardware and software, that may require modification so as to permit compliance with the provisions of this Act. A provider of common carrier support services or a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis, and at a reasonable cost, any support service or equipment, including hardware and software, which may be required so as to permit compliance with the provisions of this Act.

"**(e) Enforcement.** The Attorney General shall have authority to enforce the provisions of subsections (a), (b), (c), and (d) of this section. The Attorney General may apply to the appropriate United States District Court for an order restraining or enjoining the provision of service of any common carrier who violates subsection (a), (b), (c), or (d) of this section. The District Courts shall have jurisdiction to issue such restraining order or injunction. The Attorney General may also request the Federal Communications Commission to assist in enforcing provisions of this Act.

"**(f) Penalties.** Any common carrier that 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 penalties. After consultation with the Attorney General, the

Federal Communications Commission may also impose regulatory sanctions or fines otherwise authorized by law.

"**(g) Consultation.** The Attorney General is encouraged to consult with the Federal Communications Commission and common carrier representatives and to utilize common carrier standards bodies, associations, or other such organizations to discuss details of the requirements, such as those related to capacity, in order to facilitate compliance with the provisions of this Act.

"**(h) Funding.** Notwithstanding any other provision of law, the Federal Communications Commission shall implement promptly methods and procedures that allow each common carrier to be remunerated by the Federal Government for all reasonable costs incurred in the course of complying with the requirements of this Act.

"**(i) Definitions.** -- As used in this Section --

(1) 'common carrier' means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103-66;

(2) 'provider of common carrier support services' means any person or entity who provides services to a common carrier that are integral to processing, directing, forwarding, or completing telephone calls or electronic communication transmissions;

(3) 'wire communication' shall have the same meaning as set forth in subsection 2510(1) of title 18, United States Code;

(4) 'electronic communication' shall have the same meaning as set forth in subsection 2510(12) of title 18, United States Code;

(5) 'intercept' shall have the same meaning as set forth in section 2510(4) of title 18, United States Code, except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication;

(6) 'concurrent with the transmission of the communication,' as used in section 3(a)(2) of this Act, means contemporaneous with the transmission; but it shall include, with regard to electronic communications, the ability of a government agency to acquire such communications at the conclusion of the transmission, and, with regard to call set up information, the ability to acquire such information either before, during, or immediately after the transmission of the communication;

(7) 'call set up information' shall mean the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or

lawful authorization, including information associated with any telecommunication system dialing or calling features or services; and

(8) 'government' means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance."

SEC. 4. COMMUNICATIONS PRIVACY IMPROVEMENT AND MONITORING CLARIFICATION.

Chapter 119 of title 18 is amended by making the following changes:

(1) Cordless telephones.

(a) Definitions. - Section 2510 of title 18, United States Code, is amended -

(1) in paragraph (1), by striking ", but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (12), by striking subparagraph (A) and redesignating subparagraphs (B) through (D) as subparagraphs (A) through (C), respectively.

(b) Penalty. - Section 2511 of title 18, United States Code, is amended -

(1) in subsection (4)(b)(i), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

(2) Radio based data communications.

Section 2510(16) of title 18, United States Code, is amended by striking the word "or" at the end of subparagraph (D) and inserting an "or" at the end of subparagraph (E) and adding the following new subparagraph:

"(F) an electronic communication;".

(3) Penalties for monitoring radio communications that are not scrambled, encrypted, or non-public.

Section 2511(4)(b) of title 18, United States Code, is amended by deleting the phrase "or encrypted, then--" and inserting the following:

", encrypted, or transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication, then--".

(4) Technical correction.

Section 2511(2)(a)(i) of title 18, United States Code, is amended by striking out "used in the transmission of wire communication" and inserting in lieu thereof "used in the transmission of a wire or electronic communication".

(7) 'call setup information' shall mean available information generated which identifies, and is associated with, the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunication system dialing or calling features, "on hook" and "off hook" information, and any available facility or services number that is transmitted; except that such information shall not include any information that may disclose the physical location of the facility or services; and

balance

(1) Strike Findings

(2) Simplify and Clarify Requirements

not P.BX
not e mail carriers

- Government Monitoring Plant
- System Security
- Call Forwarding/700 Services
- Title III Language on Unobstrusiveness
- Cost Sharing

(3) Cordless Phones

(4) Radio Based Data Communications
Radio Based Laws

(5) Non Public Communications TDMA/EDMA

(6) E-Mail System Quality Monitoring]

→ main stream carriers
→ generic requirement to be built in
→ 3 years
→ remuneration
→ security feature
→ privacy enhancement
→ no encryption
→ no gov't monitoring system
→ clear statement not enhancing authority

1. clipper
2. export control
3. digital telephony

Digital Telephony Legislation

Key Provisions:

- **Finding that telecommunication networks and systems are often used in furtherance of serious and violent criminal activity, including drug trafficking; terrorism; and espionage.**

- **Advances in telecommunications technology and new technologies impede effective electronic surveillance, frustrate court orders, prevent law enforcement and intelligence agencies from discharging their duties, and imperil the public safety and national security.**

- **Without the assistance of common carriers, telecommunications equipment manufacturers, and providers of common carrier support services, such impediments will continue and increase.**

- **The stated purpose of the legislation is to clarify and define the responsibilities of common carriers, equipment manufacturers, and support service providers in meeting the electronic surveillance requirements of law enforcement.**

- **This legislation eliminates from coverage the computer-based networks and companies as well as the PBX operators which were included in last year's legislative draft. The focus of the current legislation is on "mainstream" "common" carriers-entities which traditionally have been subject to regulation.**

- **Common carriers are required to meet law enforcement electronic surveillance requirements within three years of the date of the legislative enactment.**

- **Law enforcement's electronic surveillance functional requirements are set forth generically. (There is no intent to dictate how a particular carrier achieves compliance.)**

- **Common carriers are directed to meet with manufacturers and support service providers promptly to identify equipment and software requiring modification to ensure carrier compliance.**

- **Equipment manufacturers and support service providers are required to furnish needed equipment/software on a timely and priority basis and at reasonable costs, to ensure compliance.**

- **The Attorney General and U.S. District Courts are vested with authority, respectively, to enforce and hear actions concerning this Act, including injunctive relief and civil fines. The Attorney General may also request the FCC to assist with enforcement and sanctions or fines.**

- The Attorney General is encouraged to consult with the FCC and common carriers and utilize standards bodies, associations, etc. to facilitate compliance with the Act.

- The Federal Government will remunerate common carriers for reasonable expenses incurred in complying with the Act. The costs will not be passed along to subscribers through rate or tariff increases. Though not decided, an appropriate funding channel is the FCC. Some of the cost remuneration likely can be achieved through FCC depreciation enhancements. Tax credits may also be utilized. If necessary, an increase in the FCC's budget may be required to cover remuneration not secured through administrative cost adjustments or corporate tax benefits.

K/DSRD/SUB/93-RF105/3
Limited Distribution

MARTIN MARIETTA

IDENTIFICATION AND ANALYSIS OF FOREIGN LAWS AND REGULATIONS PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION PRODUCTS FOR VOICE AND DATA COMMUNICATIONS

Professor James P. Chandler
Diana C. Arrington
Donna R. Berkelhammer
William L. Gill

January 1994

Prepared by
National Intellectual Property Law Institute and
The George Washington University
1350 Eye Street NW, Suite 820
Washington, DC 20005
Subcontract No. 19K-RF105C

DOE Project No. 2042-E024-A1

Prepared for
Data Systems Research and Development Program
Technical Operations
Oak Ridge K-25 Site
Oak Ridge, Tennessee 37831-7620
Managed by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

MANAGED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

K/DSRD/SUB/93-RF105/3
Limited Distribution

IDENTIFICATION AND ANALYSIS OF FOREIGN LAWS AND REGULATIONS PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION PRODUCTS FOR VOICE AND DATA COMMUNICATIONS

Professor James P. Chandler
Diana C. Arrington
Donna R. Berkelhammer
William L. Gill

January 1994

Prepared by
National Intellectual Property Law Institute and
The George Washington University
1350 Eye Street NW, Suite 820
Washington, DC 20005
Subcontract No. 19K-RF105C

DOE Project No. 2042-E024-A1

Prepared for
Data Systems Research and Development Program
Technical Operations
Oak Ridge K-25 Site
Oak Ridge, Tennessee 37831-7620
Managed by
Martin Marietta Energy Systems, Inc.
for the
U.S. Department of Energy
under contract DE-AC0584OR21400

CONTENTS

ABSTRACT

This document analyzes foreign controls pertaining to encryption technology. Controls surveyed include export and import laws and any domestic laws that could be found. Research for this task began with a search of actual statutes and codes of the foreign countries. This search yielded limited and incomplete information which had to be supplemented by other resources. The researchers collected information from various embassies, with limited success, and also referred to various secondary sources such as reports prepared for the National Institute of Standards and Technology for conferences addressing encryption issues. The authors of reports were called and queried as to the strength and validity of the information presented in the reports. This process proved to be rather helpful. During the analysis of the reports, it was found that others have attempted this type of research before and have had similar limited success. Twenty-one countries were researched by the aforementioned method. Information was found for most of the countries. A few countries had no official controls, although actual controls may in fact be exercised.

ACRONYMS

EIPA	Export and Import Permits Act
COCOM	Committee for Multilateral Export Controls
EC	European Economic Community

1. INTRODUCTION

This document analyzes foreign controls pertaining to encryption technology. Controls surveyed include export and import laws and any domestic laws that could be found. Research for this task began with a search of actual statutes and codes of the foreign countries. This search yielded limited and incomplete information which had to be supplemented by other resources. The researchers collected information from various embassies, with limited success, and also referred to various secondary sources such as reports prepared for the National Institute of Standards and Technology for conferences addressing encryption issues. The authors of reports were called and queried as to the strength and validity of the information presented in the reports. This process proved to be rather helpful. During the analysis of the reports, it was found that others have attempted this type of research before and have had similar limited success, with one manufacturer finally having its subsidiaries ask foreign government officials what their policies were.

Twenty-one countries were researched by the aforementioned method. Information was found for most of the countries. A few countries had no official controls, although actual controls may in fact be exercised.

2. ENCRYPTION TECHNOLOGY FOREIGN LAWS

2.1 AUSTRALIA—IMPORT CONTROLS ON ENCRYPTION TECHNOLOGY

Australia requires an import certificate for encryption software or hardware only upon request by the exporting country.[1]

2.2 BELGIUM—IMPORT CONTROLS ON ENCRYPTION TECHNOLOGY

Belgium does not impose import restrictions for encryption technology.[2]

2.3 BRAZIL—IMPORT CONTROLS ON ENCRYPTION TECHNOLOGY

Brazil does not impose import restrictions for encryption technology.[3]

2.4 CANADA

2.4.1 Export and Import Permits Act

The Export and Import Permits Act (EIPA) regulates the export and import of goods in Canada. To ensure compliance with the provisions of EIPA, customs officers are authorized to satisfy themselves that all pertinent requirements have been met.[4] The provisions of the Customs Act pertaining to search, detention, seizure, forfeiture, and condemnation apply where any provisions of the EIPA or regulations have been violated.[5] Violators are subject to criminal prosecution.[6]

2.4.2 Import Controls

Based on the listed items in the Import Control List, the importation of cryptographic technology into Canada is not controlled.[7]

---

[1] Statement of the Computer and Business Equipment Manufacturers Association, Before the Computer System Security and Advisory Board, National Institute of Standards and Technology (May 27, 1993).

[2] *Id.*

[3] *Id.*

[4] Doing Business in Canada, Import-Export § 6.10(3) (1992).

[5] R.S.C. 1985, chap. E-19, § 25.

[6] *Id.* at § 19.

[7] R.S.C. 1985, chap. E-19.

2.4.3 Export Controls

The exportation of items from Canada may be subject to restriction if they are included on the Export Control List[8] pursuant to the EIPA. Canada follows the Coordinating Committee for Multilateral Export Controls (COCOM) regulations in the regulation of cryptographic technology. Encryption devices are outlined in category five, part two of Canada's export regulations. These provisions are similar to U.S. category five in the Export Administration Regulations.[9]

2.5 PEOPLES REPUBLIC OF CHINA

2.5.1 Import Controls

China practices a licensing scheme for imported commodities. An application is to be filed and a license obtained in advance by corporations approved by the state to engage in the business of importing commodities. A license is valid for 1 year, and a corporation may apply for an extension.

Based on China's List of Prohibited and Restricted Imports and Exports enacted in 1987, China restricts the importation of voice-encoding devices.[10]

2.5.2 Export Controls

A corporation engaging in the exportation business must first file an application for approval with the Ministry of Foreign Trade or the foreign trade bureau of the province.[11] The Ministry establishes an export control list of prohibited and restricted goods.

Based on China's List of Prohibited and Restricted Imports and Exports, China restricts the exportation of voice-encoding devices.[12]

2.6 EUROPEAN COMMUNITY

In 1957, the Treaty of Rome[13] established the European Economic Community (EC). The EC members are the territories of Belgium, Denmark, the Federal Republic of Germany, France, Ireland, Italy, Luxembourg, the Netherlands, Great Britain, Greece, Spain, and Portugal. In 1986, the Single European Act[14] modified the treaties, creating the European Communities so as to

---

[8] R.S.C. 1985, chap. E-19, as amended.

[9] 15 C.F.R. pts. 768–799.

[10] Notice of the General Administration of Customs of the People's Republic of China, § 50-305 (November 1, 1987).

[11] Interim Procedures of the State Import-Export Commission and Ministry of Foreign Trade of the People's Republic of China Concerning the System of Export Licensing (June 3, 1980).

[12] Notice of the General Administration of Customs of the People's Republic of China, § 50-305 (November 1, 1987).

[13] 298 U.N.T.S. 11 (1957), art. 238 (March 25, 1957).

[14] Law No. 86-1275 (December 16, 1986).

establish an internal market without boundaries in which free dissemination of merchandise, persons, services, and capital are assured. The free internal market would be continually implemented by the member-states during the course of a 5-year period concluding on December 31, 1992.

2.6.1 Import Controls

Most articles imported from EC member-states are not subject to restrictions. The rules applicable to the free movement of goods are derived from Articles 9 et seq. of the Treaty of Rome. However, Article 36 allows prohibitions of restrictions on imports justified for various reasons, such as public morality, public policy, or public security. The EC courts have consistently held that Article 36 is applicable to measures of a noneconomic nature, such as the maintenance of a national health care system or the security of member-state oil supplies.[15]

No import/export controls on encryption technology were found.

2.6.2 Export Controls

Most products exported to EC member-states are not subject to restrictions; however, certain sensitive products and technologies deemed necessary for national policy are subject to the laws and regulations instituted by member-states.[16] The sensitive nature of certain products derives from the dual use—civil and military—which can be made of them. Intra-EC member trade is to be regulated by controls pursuant to the COCOM rules; however, a satisfactory basis for cooperation between member-states and the Commission has not been established. The objective will be to develop uniform export and import control lists of products and their respective destinations.[17] The developing momentum of the intergovernmental conference on political union in regard to exports of weapons and nonproliferation should facilitate an agreement on the treatment of dual-use products.[18]

No import/export controls on encryption technology were found.

Currently, the Commission of the European Communities is developing a European telecommunications policy to establish a common telecommunications market (networks and telecommunications equipment).[19] The emerging telecommunication policy is governed by the Treaty of Rome and by the fundamental human rights as developed by the European Court of Justice.[20] This telecommunications policy might affect the future controls on cryptographic technology in voice and data networks.

---

[15] Hansen, Paul, *Freedom of Data Flows and EC Law*, Sixth Report of the Commission, p. 7 (1988).

[16] Doing Business in France, § 16.029(5) (1988); Sixth Report of the Commission, EC and the Single Market, pp. 14–15 (1991).

[17] Sixth Report of the Commission, EC and the Single Market, p. 15 (1991).

[18] *Id.*

[19] Hansen, Paul, *Freedom of Data Flows and EC Law*, p. 85 (1988).

[20] *Id.* at p. 90.

2.7 FRANCE

2.7.1 Import Controls

Imports into France are governed by French law and the EC regulations.[21] Two considerations must be considered in connection to entry of goods into France: whether goods to be imported into France are subject to any import restrictions and what declarations or filings are to be made for permissible importation. Goods can fall into four categories: articles not subject to restrictions, articles subject to prior notification, articles subject to an import license, or articles subject to special import restrictions.[22]

Almost all goods that originate in the EC as well as certain goods specified by law may be imported into France without being subject to import restrictions. An import license is valid for only 6 months and only with reference to a specific type of merchandise coming from a specific origin.[23]

France requires a license for the import of encryption into the country.[24] France requires Data Encryption Standard–based encryption manufacturers and users to deposit a key with the French government, and they may also require an import license if it is determined necessary on a case-by-case review. France would probably forbid the use of key escrow technology unless they are given the keys and a full description of the algorithm.[25]

2.7.2 Export Controls

Most products exported to EC member-states are not subject to restrictions; however, certain products are subject to prior notification, an export license, or a prior authorization before they may be exported. Such notifications, licenses, or authorizations are obtained pursuant to similar procedures governing importations.[26]

In order to preserve the interests of French national security or defense, exports or use of cryptography must (1) be "declared prior to the operation when this operation only results in certification, or in the securization of the transmitted message; and (2) be authorized prior to the operation by the Prime Minister in any other cases."[27] The penalty for not complying is a fine of 6,000 to 500,000 FF and/or a prison sentence from 3 to 8 months.[28]

A declaration of delivery or use of means of cryptography is issued at the central bureau for security of information systems. The request form for a declaration has two parts, a technical part and an administrative part. The technical part is an "extensive description in French of the

[21] Doing Business in France, § 16.02(1) (1988).

[22] *Id.* at § 16.02(3)(a)(i).

[23] *Id.* at § 16.02(3)(a)(i)(C).

[24] Bob Rarog, *Encryption Export Controls & the Computer Industry*, Digital Equipment Corporation (May 1, 1993).

[25] Statement of the Computer and Business Equipment Manufacturers Association, Before the Computer System Security and Advisory Board, National Institute of Standards and Technology (May 27, 1993).

[26] Doing Business in France, § 16.02(5) (1988).

[27] Regulation of Telecommunications, LOI n.90-1170, art. 28(I)(a), (b) (December 29, 1990).

[28] *Id.* at art. 28(II).

operation or means of cryptography and of its exploitation mode, including the management of secret arrangements."[29] The administrative part allows for the identification of the person requesting the operation, location of the operation, and the categories of persons or societies allowed to use the operation.[30] The request indicates the duration for which the authorization is requested, which cannot exceed 10 years.[31] The export of cryptography requires the deposit of a copy of the receipt of the declaration to the customs office.

As in the United States, France has decontrolled software that is in the public domain, and it retains control of mass-market and other encryption software as military items.

2.8 GERMANY

2.8.1 German Foreign Trade Act

The German Foreign Trade Act of 1961 regulates German trade and recognizes the need to reduce to a minimum restrictions and formalities in the import and export of goods. Germany is considered one of the world's most liberal trading nations.[32] However, Germany does provide for prohibitions and restrictions for the protection of Germany's market organization, specific industries, public health, and public order.[33] Germany draws a distinction between trade regulations on the one hand and noncommercial regulations on the other. Noncommercial regulation serves a purpose that is not directly related to international trade, but rather to serving public health, safety, industry, and public order.[34] Since Germany is a member of the EC, the country's foreign trade policy has become increasingly influenced by EC legislation.[35]

2.8.2 Import Controls

Germany has an import control list over 300 pages in length which in combination with a list of countries indicates whether a license is required. A license can be applied for at the Federal Office for Commercial Business.[36]

Germany does not have any restrictions on encryption products.[37]

2.8.3 Export Controls

The Foreign Trade Ordinance contains an export control list of all goods subject to foreign trade restrictions. The export list does not impose prohibitions, but it indicates authorization

[29] *Id.* at art. 6.
[30] *Id.*
[31] *Id.*
[32] Droste, Killius, and Triebel, *Business Law Guide to Germany*, 3rd edition, CCH Editions Limited, p. 1 (1991).
[33] *Id.*
[34] *Id.* at p. 2.
[35] *Id.* at p. 4.
[36] *Id.* at p. 6.
[37] Bob Rarog, *Encryption Export Controls & the Computer Industry*, Digital Equipment Corporation (May 1, 1993).

requirements. All goods requiring authorization are classified by a four-digit code number. COCOM restrictions are incorporated into the export list.

Germany has specifically exempted encryption software from the General Software Note of the COCOM Industrial List.[38] Therefore, Germany maintains control of both public domain and mass-market encryption software.

2.9 INDIA

No import/export controls were found.

2.10 ISRAEL

Israel imposes import restrictions on encryption; however, the scope of their restrictions is not clear.[39]

2.11 ITALY

There are no import restrictions on encryption technology.[40] Italy follows COCOM regulations for the export of encryption technology, allowing public-domain and mass-market software to be exported with no license and other encryption-capable items to be exported with a validated license.

2.12 JAPAN

2.12.1 Import/Export Controls

The Foreign Exchange and Foreign Trade Control Law governs the import and export of goods in Japan. The Law is designed to permit the export of goods with minimal restrictions.[41] The Law provides for some restrictions in order to prevent unfair exportation and ensure orderly importation.[42] Unfair exportation includes the export of goods that may infringe on an industrial property right or copyright protected in the country of destination, export of goods with false representation of country of origin, and goods that greatly differ from the specifications given in the contract.[43]

---

[38] *Id.*

[39] Statement of the Computer and Business Equipment Manufacturers Association, Before the Computer System Security and Advisory Board, National Institute of Standards and Technology (May 27, 1993).

[40] Per Italian Embassy.

[41] *Japanese Law*, 425, art. 47 (1992).

[42] *Id.* at 415; Law No. 299 (1952).

[43] *Id.* at 416; art. 2.

The Law requires export licenses for certain kinds of goods and services for certain destinations.[44] A person who intends to export goods and/or technology to a destination designated in a cabinet order as an area where international peace and security are obstructed is required to obtain a license from the Minister of International Trade and Industry.[45] Primarily, restrictions involve COCOM-controlled goods and technologies. Japan joined COCOM in 1950 and enforces COCOM controls through a national list of strategic goods and technology.[46] The list is published together with other controlled items in a cabinet order and is administered by the Ministry of International Trade and Industry.[47]

2.12.2 Encryption Technology Controls

Japan follows COCOM guidelines for the export of encryption technology.[48] Generally, public-domain and mass-market software may be exported without a validated license. Other encryption technologies are reviewed on a case-by-case basis. No import controls were found. No domestic controls on encryption use were found.

2.13 SPAIN

2.13.1 Import/Export Controls

The export of goods is regulated by Royal Decree No. 2426 of September 14, 1979. Royal Decree No. 2426 regulates the processing of export transactions, payment of the purchase price, control, and the evaluation of trade balances.[49] All goods may be exported, provided the conditions and requirements set forth by the Decree have been met. There are no limitations other than those established by the government for reasons of morality, health, public order, or other internationally recognized reasons.[50] The export of goods is carried out by allowing the granting of a license by the Minister of Economy and Finance.

2.13.2 Encryption Technology Controls

No import/export controls or domestic controls were found.

2.14 THE NETHERLANDS

2.14.1 Import/Export Laws

The Import and Export Act of 1963 controls the import and export of goods. Imports and exports are free from any restrictions or registration formalities other than those expressly imposed. The

---

[44] *Id.* at 416.
[45] *Id.* at 416; art. 48; art. 25.
[46] *Id.* at 416.
[47] *Id.* at 416.
[48] Bob Ratog, *Encryption Export Controls & the Computer Industry*, Digital Equipment Corporation (May 1, 1993).
[49] Doing Business in Spain. § 16.02(3) (1987).
[50] *Id.* at § 16.02(3)(a).

Act states that restrictions and formalities may be imposed by regulations or decrees issued by the Minister of Economic Affairs or Minister of Agriculture.[51] A number of decrees and regulations have been issued. The Economic Information Service, a service of the Ministry of Economic Affairs, maintains a list of current regulations and decrees, as well as a list of those goods for which import or export licenses are required.[52]

2.14.2 Encryption Technology Controls

Annex B of the Import and Export of Industrial Goods Decree of 1963 sets forth a list of industrial products for which an export license is required.[53] The Export of Strategic Goods Decree of 1963 prohibits the export of an extensive number of products of a strategic nature.[54] Public domain and mass-market software generally does not require a validated license. Items capable of file encryption do require a validated license. No import restrictions were found.

2.15 UNITED KINGDOM

2.15.1 Import/Export Laws

The Import, Export and Customs Powers (Defence) Act of 1939 governs the import and export of goods in the United Kingdom. The Department of Trade and Industry regulates the import and export of goods. Generally, the United Kingdom follows COCOM guidelines for the export of COCOM-controlled goods.

2.15.2 Encryption Technology Controls

The United Kingdom controls encryption items as dual-use items. No license is required for the export of mass-market and public-domain software. Other encryption items may be granted export licenses on a case-by-case basis. No import controls were found for encryption technology.

2.16 SOUTH AFRICA

2.16.1 Import/Export Laws

The Import and Export Control Act, No. 45 of 1963, governs imports and exports in South Africa. The minister of Trade and Industry and Tourism has regulatory control over exports and imports. South Africa reserves the right to control or prohibit the export of certain goods from its country. Generally, prohibited exports consist of arms and ammunition.

---

[51] *Dutch Business Law*, § 28.02(1) (1990).
[52] *Id.* at § 28.02(1); § 28.04(1).
[53] *Id.* at § 28.04(2)(a).
[54] *Id.*

2.16.2 Encryption Technology Controls

No controls exist on the export of encryption technology.[55] South Africa generally shapes its export practices to the import laws of the importing country. No import restrictions were found.

2.17 RUSSIA

No import or export restrictions were found.

2.18 SAUDI ARABIA

No import or export restrictions were found.

2.19 MEXICO

The Mexican Institute of Foreign Trade governs imports and exports in Mexico. No export or import controls were found on encryption technology.

2.20 SWEDEN

No import or export restrictions on encryption technology were found.[56]

2.21 SWITZERLAND

No import or export restrictions on encryption technology were found.[57]

---

[55] Per South African Embassy.
[56] Bob Rarog, *Encryption Export Controls & the Computer Industry*, Digital Equipment Corporation (May 1, 1993).
[57] *Id.*

DIGITAL TELEPHONY LEGISLATION
Cost estimates for FY 95, FY 96, and FY 97 Federal Budgets

Summary: It is infeasible to give a hard and accurate estimate of the costs which the federal government will incur in remunerating common carriers for the charges they will incur during the three-year period which is set for compliance. Since common carriers, to date, have not been put in a position where they have had to explore precisely and in-depth the exact types of, or levels of complexity associated with, technical modifications, specifications, and likely software and hardware alterations required, we can only proceed by furnishing a rough order of magnitude (ROM) estimate of a possible range of costs. There are innumerable variables; but, if a moderately aggressive deployment of needed modifications were made throughout the telecommunications networks, the costs **could be** within a range of $300-$500 million. It is believed that firm and accurate figures can only be obtained once common carriers, acting pursuant to a statutory mandate, discuss with the government the in-depth details of the technical and "feature" specifications which each common carrier will develop in order to make its network compliant.

Details: As all are aware, a policy decision was made some time ago that the government would not seek to "dictate" precise technical solutions or tell common carriers how to respond technically to the government's electronic surveillance requirements. Today, there are roughly 2,000 common carriers. Each carrier's network is somewhat unique. The networks of a number of carriers already accommodate court-ordered electronic surveillance and will require little or no modification. The larger portion, however, will require modifications. The depth and breadth of the modifications required will vary widely, and the specific technical approaches and business alliances these carriers will pursue to meet these requirements also will vary.

In an effort to achieve the most efficient cost-effective solutions industry-wide, the legislation includes several provisions which are designed to keep costs under control:

a) the Government will <u>consult</u> with common carriers to "discuss details of the requirements...and cost-effective approaches, in order to facilitate compliance..." (Section 3(g))

b) the Government will pay common carriers for "reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance" (Section 3(h))

c) "common carrier support service providers and telecommunications equipment manufacturers shall make [services and equipment] available to common carriers at a reasonable and cost-effective charge..." (Section 3(d)

d) the Attorney General has the authority to enforce the foregoing provisions. (Section 3(e))

Although the government does not intend to dictate solutions, nevertheless, it intends, under the "consultation" provisions of the legislation, to use industry standards bodies, associations, and other such organizations as likely "clearing houses" for promising, cost-effective technological approaches and solutions. We believe such efforts will reduce more costly and duplicative independent efforts on the part of each carrier. Close follow-up consultation is also envisioned when the technical and feature specifications are being crafted to avoid mistakes and misunderstandings.

Assumptions:

- For planning purposes, we are assuming that the charges that the federal government will incur will mostly occur within federal government Fiscal Years 1995-97.

- Most likely, new technologies and services will be introduced during the three-year compliance period. (Our revised ROM estimate of the range of charges has been affected, in part, by the earlier-than-anticipated deployment of personal communications services (PCS) and the recent, unanticipated mergers within the telecommunications industry (e.g., Bell Atlantic-TCI). Such unforeseen circumstances have added to the near-term technological complexity of the telecommunications marketplace.) At the conclusion of the compliance period new technologies and services introduced will be expected to comply without costs incurred to the government.

- Some services offered by common carriers currently meet law enforcement requirements and therefore modifications are not necessary. Consequently, the government should incur little or no charges regarding such common carriers.

- There is anecdotal information that certain switch manufacturers and common carriers currently are developing (or have developed) partial solutions which satisfy some of the electronic surveillance requirements.

o Different common carriers will choose different means to meet the government's requirements. Therefore, the costs associated with complying with the requirements will vary greatly depending on the course of action taken by each common carrier. (Efforts will be made by government to facilitate, whenever possible, common cost-effective approaches in order to reduce costs.

o Costs associated with achieving compliance are increasing daily. Therefore, with the passage of time over the next three years, costs will rise beyond estimates previously made. (By meeting with industry technical committees over the last two years without achieving implementation of the technical solutions, time was lost, and the costs of attaining common carrier compliance have increased.)

ROM Estimated Costs

It is infeasible to give a hard and accurate estimate of the costs which the federal government will incur in remunerating common carriers for the charges they will incur during the three-year period which is set for compliance. Since common carriers, to date, have not been put in a position where they have had to explore precisely and in-depth the exact types of, or levels of complexity associated with, technical modifications, specifications, and likely software and hardware alterations required, we can only proceed by furnishing a ROM estimate of a possible range of costs. **The actual costs for meeting law enforcement's requirements and complying with the legislation can only be derived by common carriers as and when the solutions are developed and the modifications deployed.**

Common carriers are in the best position to identify solutions and ensure the proper implementation of solutions into their networks. Once legislation is passed, it is expected that follow-up meetings with the government to discuss the details for implementing proposed industry solutions will more precisely identify costs. Once this occurs, a number of alternatives may be selected by industry to meet law enforcement's requirements and comply with the legislation. Depending upon the technology, a common carrier may elect to design a solution based upon existing commercial products. In this case, incurred costs would likely include the design of the solution, the purchase of the identified products, installation, and then testing. Another alternative is for the common carrier to specify requirements of a new feature to be implemented in the carrier's switching and/or control systems.

Given the complexity of the telecommunications network, a common carrier is likely to employ a mixture of these strategies based on the characteristics of their network and the strategic business goals of the company. Discussions with industry have indicated that possible solutions would probably affect a number of switching and other network elements. This would include both wireline and wireless technologies. If 20,000 of the potential 24,000 switches and/or other network elements were targeted, the costs to address law enforcement's concerns could range from $300 million to $500 million. These costs could vary greatly depending on the actual number of affected network elements and the costs associated with developing these features.

If an approach is selected that mirrors conventional "commercial" feature packages and upgrades, the costs are likely to be somewhat comparable to other commercial switch software and network products. On the other hand, to the extent that direct discussions among common carriers, equipment manufacturers, support service providers, and the government can occur, there may be opportunities to reduce costs for these unconventional and "noncommercial" technical and feature solutions.

Fiscal Year:	95	96	97
Percentages: (of total costs)	5%	20%	75%

It is expected that the first-year expenses would be minimal as many common carrier activities would be devoted to planning and development of feature documents. Second-year costs are also anticipated to be low, as most of the efforts will be generally involved with the actual feature design and development by manufacturers. Third year costs will reflect the majority of the incurred expenses, as common carriers procure and implement the law enforcement features and request reimbursement for their expenditures.

Again, it must be emphasized that costs to comply with this legislation could vary greatly from this ROM estimate depending upon the solutions employed. Common carriers will be in the best position to identify the costs associated with compliance and can develop the most efficient and cost-effective strategy for addressing law enforcement needs by working with the government to further define solutions and implementation strategies.

SECTION BY SECTION ANALYSIS

Section 1. Short Title

Section 1 provides that the short title of the Act is the "Digital Telephony and Communications Privacy Improvement Act of 1994."

Section 2. Purpose

Section 2 states the purpose of the Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information (e.g., dialed number information) pursuant to the Federal and state electronic surveillance and pen register and trap and trace statutes. An effective electronic surveillance capability is essential to Federal, state, and local agencies so that they can secure the public safety, effectively enforce the law, and maintain the national security. Without clarification of the increased responsibilities of the telecommunications industry to assist and cooperate, this critical investigative technique will be eroded, if not precluded, by the advances in telecommunications technology.

The statutory requirement for common carriers and others to provide needed assistance to law enforcement agencies in the execution of electronic surveillance court orders and lawful authorizations is a long-standing one. Since 1970, the assistance of common carriers and others has been mandated. In a 1970 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), Congress enacted a provision specifying that a "communication common carrier [common carrier], landlord, custodian, or other person shall furnish [the government applicant for court-ordered electronic surveillance] forthwith all information, facilities, and technical assistance necessary to accomplish the interception ...." In return for providing the information, facilities, and technical assistance, the assistance provider is required to be compensated by the applicant for reasonable expenses incurred in providing the assistance. See 18 U.S.C. 2518(4).

The foregoing "assistance" provision also has been incorporated in the Foreign Intelligence Surveillance Act of 1978 (FISA) (codified at 50 U.S.C. 1805(b)(2)(B)) and in the pen register/trap and trace provisions of the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. 3134(a),(b)).

The purpose of the legislation is to clarify and define the <u>nature</u> and <u>extent</u> of this responsibility which arises from the stark mandate of the foregoing laws.

In 1970, the telephone industry was monolithic, and the part of the telecommunications network where government effected electronic surveillance was relatively uncomplicated. Since that time, with the breakup of AT&T through divestiture, the entry of numerous new communications providers in the telecommunications marketplace, and the introduction of many new (and often proprietary) technologies, services, and features, the telecommunications networks have become more varied, advanced, and complicated. Though unintended, the complexities of the telecommunications networks create, and will continue to create, impediments to Federal, state, and local government agencies as they attempt to execute electronic surveillance and pen register and trap and trace court orders and authorizations.

With the passage of the ECPA amendments to Title III, electronic communications have received statutory privacy protection as well, and the term common carrier has been replaced with the broader terminology of provider of wire or electronic communication service. However, intercepting voice communications and acquiring the attendant dialing information remain of the greatest importance to government agencies; and the principal area where technological impediments have been encountered is within the networks of wireline and cellular common carriers.

Solutions have not always been readily available for existing problems, and they may not be for the future problems that are foreseen in the emerging technologies, services, and features. Such solutions also take time and may require significant "capital" outlays. As a result, industry and government agencies have been uncertain as to the nature and extent of the foregoing "assistance" provision. In particular, key questions exist in terms of who is responsible for efforts to remove the impediments; how quickly the impediments should be removed; what the consequences are, if any, for not removing them in a timely fashion; and who is responsible for paying the costs.

Because of concerns about compromising investigations, harming law enforcement and common carrier relationships, and due to the prospect of substantial delays, government agencies have been reluctant to pursue contempt or other legal remedies to resolve this issue. Also, because of the variety of technological impediments and the differences in levels of effort required to remove them, the government has been concerned that a particular judicial ruling may have only limited precedential value. Consequently, as things now stand, common carriers and other communications service providers ultimately decide what they will do to remove technological impediments, and when. When carriers and providers have acted, it frequently has taken months, and in some instances years, for ad hoc technical solutions to be developed, and the rate and breadth of their deployment have been uncertain. Thus, since the mid-1980s, technological impediments have frustrated, in whole or in part, the execution of a number of court orders for electronic surveillance, pen registers, or trap and traces, while the means of approaching and resolving the overall problem of the negative impacts of advanced telecommunications technology on electronic surveillance has eluded government and industry.

It has been observed that while it may be somewhat difficult and expensive to remove some existing impediments forthwith, that where new, advanced services and features are still under development or where upgrades are being prepared that technological solutions could be applied with significantly less difficulty and expense. Additionally, some common carriers, especially those who only more recently have entered the marketplace, have noted that they are not familiar with all of the electronic surveillance requirements of government agencies. Finally, some common carriers have stated that they rely on certain support service providers and equipment manufacturers to provide telecommunications service, and that without the help of those entities they may be unable to make the modifications required to remove the impediments and meet the requirements of government agencies.

Although Government and industry have made efforts to resolve this problem, after several years of discussion and consultation, the basic concerns and issues remain: what are the requirements of government agencies in this area; who is responsible for removing the impediments that impact on these requirements; how quickly must these requirements be met; what are the consequences, if any, for not meeting them on a timely basis; and who is responsible for paying the costs. This legislation addresses and resolves these concerns and issues.

The "Purpose" section also indicates that, excepting section 4, the legislation is not intended to alter any provision in the Federal electronic surveillance, pen register, or trap and trace statutes, or those of any state or other jurisdiction, such as those regarding the authority to intercept communications or install or use pen register and trap and trace devices; the current duty to provide assistance and receive payment therefor; causes of action; civil liability; or good faith defenses. The underlying purpose of the legislation is to clarify and define the responsibilities of common carriers such that government agencies can <u>maintain</u> their ability to properly and effectively execute electronic surveillance-related court orders and lawful authorizations.

An additional purpose to the Act, as set forth in section 4, is to improve communications privacy protection for users of cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

Section 3. New Section

Chapter 109 of title 18, U.S.C. is amended by adding a new section, section 2237, entitled: "Common carrier assistance to government agencies." Amendment of this chapter is made in order to avoid having to amend three separate, yet interrelated, Federal statutory regimes: Title III (18 U.S.C. 2510 et seq.); FISA (50 U.S.C. 1801 et seq.); and the pen register and trap and trace provisions of the ECPA (18 U.S.C. 3121 et seq.).

Common carrier assistance:
3a. Assistance requirements

Section 3(a) sets forth the requirements of government agencies when conducting electronic surveillance and pen register and trap and trace investigations. These requirements, which are generic in nature, were developed by the FBI and include input from representatives of various Federal, state, and local law enforcement agencies that utilize electronic surveillance extensively. These requirements relate to the capabilities needed to accomplish effectively the interception of communications and the acquisition of call setup information. The Government intentionally has eschewed setting any technical standards because it does not desire to "dictate" particular technological solutions. Further, owing to the diversity (and often proprietary nature) of each carrier's network and the variations in approaches that can be taken to achieve compliance, it is the Government's position that each common carrier is best positioned and qualified to determine how it will meet the requirements in the most cost-effective way.

Although the requirements set forth in section 3(a) constitute the first legislative listing of the government's requirements, the FBI states that for many years most, if not all, of these requirements have been known to the security offices of the major local exchange carriers, interexchange carriers, and cellular carriers. (Security offices usually are designated by common carriers to receive service of the court orders and authorizations and to provide law enforcement agencies with the information and assistance required to execute the court orders and authorizations.)

The legislation requires common carriers to provide "forthwith" the capability and capacity necessary to permit the government to conduct electronic surveillance, pen register, and trap and trace investigations effectively. The requirement of providing assistance "forthwith" is not new. It is found in the current language of 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805 (b)(2)(B). The language concerning capability and capacity is included to underscore the need for a common carrier to afford not only an ability to effect the interception of communications and the acquisition of call setup information (which includes dialed number information) but also the ability to accommodate without delay all court orders and authorizations for electronic surveillance, pen registers, and trap and traces that may be served on such common carrier by the various Federal, state, and local government agencies.

Within section 3(a)(1), it is stated that the foregoing capability and capacity must accommodate the "expeditious" and "simultaneous" execution of all court orders and authorizations. Frequently, it is essential to implement the interception of communications or acquire dialed number information expeditiously in order to obtain information critical to saving lives, making arrests, and seizing evidence and contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The capability and capacity requirement is also very important inasmuch as a number of government agencies must be able to execute a number of court orders and authorizations simultaneously. The FBI states that over the past decade a number of court orders and authorizations were not fully executed, or were not even sought, because of certain technological impediments and capacity shortfalls, such as insufficient "port" capacity in the cellular mobile switching offices (MSOs). At any particular time a number of Federal, state, and local government agencies may be competing to execute electronic surveillance and pen register court orders regarding certain telecommunication facilities, the access point for which is of limited capacity. Inasmuch as communications interceptions and dialed number acquisitions increasingly will be activated from within common carrier premises, including switching offices, it is critical that there be sufficient capacity to accommodate completely the concomitant needs of all government agencies.

As discussed below with regard to section 3(g), since common carriers' technological responses to the requirements will vary by common carrier and by the technology being addressed, and because historically each carrier has been subject to varied numeric demands in terms of court orders or authorizations, the Government intends to consult with common carriers and telecommunications industry representatives in a number of areas, such as in the area of capacity, in order to assist in facilitating proper sizing approaches and cost-effective compliance. Further, it is expected that most common carriers can ensure compliance in the future and gauge the future demands of government agencies by reviewing their records as to the numbers of, and trends in, current and past court orders and authorizations and extrapolating therefrom the sizing required to meet future demands. Finally, the increasing availability of "modular" and incremental technical approaches will allow common carriers to respond flexibly throughout their networks to the demands of government agencies in a cost-effective manner.

Section 3(a)(2) specifies that common carrier networks must afford government agencies an ability to intercept communications and acquire call setup information "concurrent" with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or authorization, to the exclusion of communications or information concerning any other subscriber, and without regard to the mobile nature of the subject subscriber's facility or service or the use by that subscriber of any custom features or services offered by the common carrier.

It is important that government agencies can intercept communications concurrent with the transmission of the original communication. Further, the associated requirement of being able to acquire call setup information concurrent with the subject transmission also is essential. For example, it is critical for government agencies to be able to intercept communications as they occur so they can respond immediately to life-threatening circumstances and react promptly and effectively to criminal activity in terms of making needed arrests, seizing evidence, and interdicting contraband, such as drugs, illegal weapons, bombs and other explosive devices.

The separation of signaling transmission paths from communications paths also can impede government agencies who must be able to associate the intercepted communication with the calling or called party. Aside from the negative evidentiary impact caused, this circumstance can hamper government agencies in their efforts to effectively "minimize" the monitoring and recording of non-criminal communications. Consequently, there is a requirement that common carriers can assure that call setup information will be available "concurrent with the transmission of the communication" that is the subject of the court order or authorization.

Owing to the varying availability of contemporaneous call setup information, the definition of "concurrent with the transmission of the communication" found in section 3(i)(6) specifies that the "concurrence" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communication. It is the clear preference of government agencies that common carriers will attempt to afford the ability to acquire this information before the transmission of the communication whenever reasonably feasible. Similarly, because of the difficulty of intercepting certain "electronic communications" concurrent with their transmission, the foregoing definition states that providing government agencies an ability to intercept such information at the conclusion of the transmission will satisfy the requirement.

The requirement that government agencies will have the ability to isolate the communications and call set up information of the subjects of electronic surveillance to the exclusion of the communications and call setup information of other subscribers is a basic and a long-standing one. Government agencies do not want to be faced with the prospect of having to "sort through" a tangle of communications which include those of innocent individuals who have the misfortune of having their communications "bundled" or otherwise commingled with those of the interception subject in the telecommunication transmission process. This requirement is being challenged by the increased use of digital transport, multiplexing, and fiber optics closer to the premises of the interception subject. Hence, common carriers must assure that there are means to access and isolate communications and call setup information, yet in a fashion that does not compromise the interception or acquisition effort.

The increasingly mobile nature of telecommunications facilities and service also has created impediments to the effective execution of electronic surveillance. With today's cellular telephony, communications can be "handed off" within and between networks and can be routed about such that they bypass interception access points, even when they are established within the premises of a cellular common carrier. It is believed that the communication interception and call setup information acquisition requirements of government agencies can be met by common carriers affording mobile service by drawing upon existing technologies and programming and routing capabilities and by coordinating efforts with other mobile carriers. This same requirement also has application to other mobile features and services which permit subscribers to program or otherwise direct communications to any facility designated by the subscriber (e.g., "follow me service"), as well as to the emerging mobile services encompassed in personal communications services (PCS) and other radio frequency-based mobile communications services.

Section 3(a)(2) specifies that the communication interception and call setup information acquisition requirement includes an ability to obtain such communications and information notwithstanding the use by the subject subscriber of any telecommunications custom "features" offered by the common carrier. The most notable feature impediment to effective electronic surveillance is "call forwarding." This feature permits a subscriber, whose telecommunications facility (and telephone number) is the subject of a court order or authorization, to redirect in-coming calls from that facility to other facilities. Such call redirection can be accomplished according to established programs or even randomly and dynamically. In the past, government agencies frequently have proceeded by securing additional court orders for those new facilities to which the calls have been "forwarded" or redirected by the subject subscriber of the court order or authorization. This circumstance has resulted in government agencies having to obtain more court orders or authorizations than typically would have been required; in criminal communications escaping timely interception; and, in some instances, in additional households unnecessarily becoming targets of electronic surveillance.

Section 3(a)(3) includes the requirement that there be an ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service. This language mirrors language currently found in 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B), and it is intended to prevent subjects of electronic surveillance and pen register and trap and trace investigations and others from detecting the surveillance effort.

Section 3(a)(4) contains the requirement that, once intercepted or acquired, the government agency would be able to receive the communication or call setup information in a generally available format at a location identified by the government agency distant from the subject's facility, from the interception or acquisition access point, and from the premises of the common carrier. This requirement is not new and is intended to maintain the current ability of government agencies to monitor, record, minimize, and otherwise properly administrate electronic surveillance and pen register and trap and trace investigations. This requirement is fundamentally important, since without it the safety of law enforcement officers and government employees would be put at risk, the interception or acquisition effort easily could be compromised through detection, and the effective execution of the surveillance search would be significantly disrupted.

Currently, once access has been obtained within the local loop or the common carrier's central office facilities, the communications and call setup information are transmitted back to the law enforcement agency's facility or monitoring plant, usually within the agency's office. The transmission most frequently occurs via line facilities provided by the common carrier.

The language which states that the communications and call setup information are to be received in a generally available format is intended to make clear that government agencies do not expect common carriers to translate digital transmissions to analog, etc. before affording transmission to them. Rather, it is expected that a common carrier would utilize a transmission format that was consistent with that of the communication being intercepted or acquired at the time of access, such as analog voice channel on a local loop, D4 formatted T-1 circuit, ISDN Primary Rate Interface circuit, etc. On the other hand, government agencies understand that they, not the common carriers, are responsible for processing the communications intercepted and the call setup information acquired.

Section 3(a)(4) also indicates that in some emergency or exigent circumstances that a government agency by necessity may have to access and monitor communications or dialed number information on the common carrier's premises. Government agencies understand that common carriers are not desirous of having government personnel carry out all aspects of a surveillance on common carrier premises, and it is understood that the government's presence in common carrier premises should only occur in emergency or exigent circumstances. Also, government agencies are not expecting common carrier personnel to assist in the monitoring aspects of executing a court order or authorization.

Section 3(b) specifies that government agencies shall notify common carriers of any wire or electronic interceptions or any call setup acquisitions that are to be effected within the premises of such common carrier pursuant to court order or authorization. Common carriers are required to designate individuals to activate such interceptions or acquisitions. These individuals are required to be available at all times to activate the interceptions or acquisitions. The requirement can be met by such individuals being "on call," in order to promptly respond to governmental needs as necessary. The requirement does not mean that the designated individuals actually must be on the premises at all times or that 24 hour-a-day work shifts must be established. Such interceptions or acquisitions may be activated only by the affirmative intervention of such individuals.

This provision recognizes that the access point for intercepting communications and acquiring call setup information increasingly will originate within common carrier premises. Such premises include buildings, switching offices and facilities, and network elements (e.g., signaling transfer points) maintained by the common carriers. Since it is important that these facilities, as well as the entire telecommunications network, remain secure, it is a requirement that all such access be initiated directly only by individuals designated by the common carrier.

Government agencies are not seeking the authority or ability to remotely activate interceptions within the premises of a common carrier in a fashion that bypasses personnel designated by common carrier. All executions of court orders or authorizations which require access to the switching facilities or other premises will be made <u>through</u> the individuals authorized and designated by the common carrier. Activation of interceptions or acquisitions originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the common carrier, depending upon the amount of assistance the government requires.

Section 3(c) states that to the extent common carriers providing service within the United States currently cannot fulfil the requirements set forth in subsection (a), they shall fulfil such requirements within three years from the date of enactment of the Act. This section makes clear that the focus of compliance is on common carriers within whose networks most of the electronic surveillance occurs.

Nearly all wireline and wireless voice communications are provided by local exchange carriers, interexchange carriers (and increasingly by service "resellers" and competitive access providers (CAPS)), and by cellular carriers (and soon by providers of Personal Communications Services (PCS) and satellite-based mobile communications providers). These entities are common carriers, and historically they have been subject to regulation. Since most electronic surveillance is effected within the networks of common carriers, the coverage has been scaled to focus only on those service providers within whose networks the core technological problems exist.

Although certain categories of electronic communication service providers (e.g., PBX and computer network operators) who currently have assistance responsibilities under Federal and state laws are excluded from the provisions of this legislation, nevertheless it is expected that such providers will continue to fulfil their statutory responsibilities and undertake voluntarily to accommodate the electronic surveillance needs of government. If significant technological impediments arise within their networks in the future due to inattention to government requirements or due to inaction in addressing them, consideration would have to be given to seeking expansion in the coverage of the instant legislation to include such entities.

The language of the section is also intended to indicate that common carriers still must fulfil their assistance responsibilities under 18 U.S.C. 2518(4), 3124, and 50 U.S.C. 1805(b)(2)(B) by furnishing requested information, facilities, and technical assistance, to the extent possible, during the three year grace period set for compliance. There should be no relaxation in common carrier efforts to assist government agencies in effectively executing court orders and authorizations.

Some common carriers, such as "resellers" and competitive access providers (CAPS), either may not own any equipment or facilities or the equipment or facilities they own may be such that they are not capable of effecting interceptions or acquisitions under this Act. In such cases, it is expected that such service entities would rely on the compliance of the common carrier whose facilities they lease, etc., and that they likely would seek from such common carrier legal assurances that compliance will be achieved within the statutory compliance period or that such common carrier would indemnify them for any liability or penalty they may incur if compliance is not met. If a common carrier leases a portion of its switching or other network facilities to an end user and such facilities are not under the carrier's control, then the carrier shall not be obligated to make that portion compliant as long as it remains beyond the common carrier's control.

The date for common carrier compliance is set at within three years from the date of enactment of the Act. The Government believes that this is a reasonable period within which the needed technological solutions can be identified, tested, and deployed within the networks of common carriers. As discussed below, common carriers receive important assistance and cooperation of equipment manufacturers and common carrier support service providers so that timely compliance can be achieved.

The coverage of compliance includes needed modifications to existing systems and networks (embedded base) as well as to future systems and networks (those fielded after the three year compliance period).

Section 3(d) provides that common carriers shall consult in a timely fashion with providers of common carrier support services and telecommunications equipment manufacturers so that any needed modifications to services and equipment, including hardware and software, can be made, and thus help to ensure common carrier compliance within three years. This section further specifies that a provider of common carrier support services and a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis, at a reasonable and cost-effective charge, any support services or equipment required so as to permit compliance with the provisions of the Act. The responsibilities of common carrier support service providers and equipment manufacturers are added to the legislation to indicate that they have an important role in ensuring that court orders and authorizations are not frustrated.

Assistance and cooperation from support service providers and equipment manufacturers are increasingly important, as services and equipment become more sophisticated and as common carriers rely on "outside" companies to provide them with these components. Although the direct burden of compliance falls on common carriers, nevertheless statutory responsibilities are conferred upon these support service providers and equipment manufacturers without whose help the common carriers likely could not comply. One of the major objections to the compliance date and attendant penalty provisions raised in the past by representatives of the Regional Bell Operating Companies (RBOCs) was the concern that local exchange carriers must rely on equipment manufacturers and others in order to meet many of the requirements.

Under provisions of the Modified Final Judgment (MFJ) of the consent decree regarding the Government's antitrust case against AT&T, local exchange carriers are precluded from engaging in telecommunications equipment manufacturing. However, a Department of Justice memorandum concludes that Judge Greene's order would not be an impediment to a common carrier's effecting limited, noncommercial modifications to network facilities, services, or equipment, the sole purpose of which would be to prevent the frustration of statutorily-based court orders and authorizations designed to ensure effective law enforcement, the public safety, and the national security.

Section 3(e) states that the Attorney General of the United States shall have the authority to enforce the provisions of subsections (a), (b), (c), and (d) of section 3. In order to avoid disparate enforcement actions throughout the country in ways that could be burdensome for common carriers, the responsibility for enforcing these provisions is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.

In particular, the Attorney General is specifically given the authority to apply to an appropriate United States District Court for an order restraining or enjoining the provision of service by any common carrier who violates the foregoing subsections of section 3. Similarly, to ensure common carrier compliance, the Attorney General may apply for an order, such as a writ of mandamus, which mandates the cooperation of a provider of common carrier support services or a telecommunications equipment manufacturer pursuant to the provisions in subsection (d). The intent is that there be no excuse offered by common carriers that they cannot comply because of unresponsiveness on the part of such support service providers and equipment manufacturers. The Federal district courts are specifically given jurisdiction to issue such orders. Additionally, the Attorney General may request the Federal Communications Commission (FCC) to assist in enforcing provisions of the Act. This provision recognizes the wide-ranging authority of the FCC over common carriers and others in the telecommunications industry.

Section 3(f) specifies that any common carrier that violates section 3(a) shall be subject to a civil penalty of $10,000 per day for each day in violation. The Attorney General is authorized to file a civil action to collect, and the Federal district courts have jurisdiction to impose, such fines. The FCC may also impose regulatory sanctions or fines authorized by law.

Section 3(g) provides that the Attorney General is encouraged to consult with the FCC and common carrier representatives and to utilize common carrier standards bodies, associations, and other such organizations to discuss details of the requirements, such as those related to capacity, in order to facilitate compliance with the provisions of the Act. This subsection evidences an intention on the part of Government to help common carriers achieve compliance with as little difficulty as possible, and in the most cost-effective way possible. Through detailed discussions, narrow and technical questions from common carriers can be answered and other concerns addressed.

Such fora also may act as potential clearinghouses for promising, cost-effective technological approaches and solutions, which would likely reduce costly and duplicative independent efforts on the part of each common carrier. The FBI and other law enforcement agencies have been meeting with industry (largely common carrier) technical committees for nearly two years in this regard, currently under the auspices of the Alliance for Telecommunications Industry Solutions' Electronic Communications Service Provider Committee (ECSPC). However, because of the voluntary basis and elective nature of participation in and commitment to this body, its lack of authority to require the implementation of solutions or to assign funding responsibility, and given that there is no clear legal mandate to fulfil government's requirements on a timely basis, these committees have not been effective to date in engendering the development, let alone the implementation, of the required solutions. With legislation mandating future compliance and addressing funding concerns, it is reasonable to assume that common carriers and others will utilize such committees in a more meaningful and beneficial fashion.

Section 3(h) states that the Federal Government shall pay common carriers for reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance with the requirements of this Act which are incurred within the three year period set for compliance.

The Federal Government has concluded that it should compensate common carriers for reasonable and cost-effective charges associated with devising and implementing the modifications required which remove the technological impediments and assure common carrier compliance with the government's requirements established in section 3(a). The remuneration covers charges incurred within the three year period set for compliance with regard to certain interim solutions to remove the impediments that most concern the Government; for the cost of modifying existing networks, services, facilities, and features; and for research and development and testing efforts associated with making future networks, services, and features compliant with the government's requirements. Once solutions have been identified, it is expected that they would be incorporated into successive generations of service and, where feasible, into new services without additional charge to the Government.

Section 3(i) sets forth definitions for sections 1-3 of the Act. The term "common carrier" means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103-66. This definition encompasses such service providers as local exchange carriers, interexchange carriers, service "resellers," competitive access providers (CAPS), cellular carriers, personal communications services (PCS), satellite-based service providers, and any other common carrier who offers wireline or wireless service to the general public.

The term "provider of common carrier support services" means any person or entity who provides services to a common carrier that are integral to processing, directing, forwarding or completing telephone calls or electronic communication transmissions. There are currently over one hundred such support service providers that provide common carriers with specialized support services.

The terms "wire communication" and "electronic communication" have the same meanings as set forth at 18 U.S.C. 2510(1) and 2510(12), respectively, under Title III, as amended by the ECPA.

The term "intercept" has the same meaning as set forth at 18 U.S.C. 2510(4), except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication. The term "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication...." The term "contents" includes "any information concerning the substance, purport, or meaning of [a]... communication." 18 U.S.C. 2510(8). The language in the definition of "intercept," as used in this legislation, is intended to clarify that a common carrier has no obligation to decrypt communications that have been encrypted by the subscriber, such that the conversation or data transmission can immediately be understood by the government, unless the encryption was provided by the common carrier and the carrier possesses the information necessary to decrypt the communication.

The term "concurrent with the transmission of the communication" means contemporaneous with the transmission of the communication, but it also includes, with regard to electronic communications, the ability of the government to acquire such communications at the conclusion of the transmission, and, with regard to call setup information, the ability to acquire such information either before, during, or immediately after the transmission of the communication.

The definition of "concurrent with the transmission of the communication" found in section 3(i)(6), is somewhat broader than term might imply on its face. The definition was broadened due to the varying feasibility of effectively intercepting electronic communications contemporaneously and the varying availability of call setup information contemporaneous with the transmission of the communication with which it is associated. Because of the difficulty of intercepting certain electronic communications concurrent with their transmission, the foregoing definition states that providing an ability for government agencies to intercept such information at the conclusion of the transmission will satisfy the requirement. The definition also specifies, with regard to call setup information that the "concurrence" requirement is satisfied if such information can be acquired by government agencies either before, during, or immediately after the transmission of the communication. It is the clear preference of government agencies that common carriers will attempt to assure an ability to acquire this information before the transmission of the communication whenever reasonably feasible.

The term "call setup information" means the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunications system dialing or calling features or services. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted. In pen register investigations, these are the pulses, tones, or messages which identify the numbers dialed from the facility that is the subject of the court order or authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization.

With regard to electronic communications, the information is that generated during the establishment of communications or the transmission of a protocol data unit, such as a datagram, that identifies the origin and destination of the communication. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as the header of a frame or packet.

The call setup information also encompasses numbers identified incidental to calls where calling features or services are used.

The term "government" means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance.

Section 4. Communications Privacy Improvement and Monitoring Clarification.

Section 4 includes several amendments to Chapter 119, United States Code, which includes Title III, with regard to communications privacy improvements and clarifications concerning monitoring of electronic communications.

In section 4, amendments are made to the definitions found in 18 U.S.C. 2510(1) and (12). The purpose of the amending language is to provide communications privacy protection to cordless telephone communication transmissions occurring in the radio link between the telephone handset and base station.

Because of the ease with which communications occurring in the radio portion of cordless telephone transmissions could be overheard through the use of commercial radio receivers, scanners, and similar cordless telephones operating in the same area, Congress chose not to confer statutory privacy protection upon the radio portion of cordless telephone communications or to criminalize the interception of same in the 1986 ECPA amendments to Title III. However, since then, advances in cordless telephony have resulted in the mass-marketing of various types of cordless telephones, many of which are considerably more difficult to intercept than the earlier models. Because newer versions and types of cordless telephones incorporate features and technology that typically afford greater security to the user, there now exists a basis for providing full statutory privacy protection to cordless telephones. Even absent the prior statutory privacy protection, the view that certain cordless telephone users nonetheless retain Fourth Amendment privacy protection under the "reasonable expectation of privacy" criteria has been asserted. See United States v. Smith, 978 F.2d 171, 176 (5th Cir. 1992). This amendment now confers the same communications privacy protection for the millions of cordless telephone users as is currently afforded to cellular telephone users.

The penalty provisions for intercepting cordless telephones are also made consistent with those for intercepting cellular telephones, by the amendments to 18 U.S.C. 2511(4)(b)(i) and (ii) set forth in this section.

Section 4 also includes language which amends 18 U.S.C. 2510(16), communications deemed to be "readily accessible to the general public" with regard to radio communications, and the exceptions thereto. The excepted categories currently covered under section 2510(16)(A)-(E) enjoy privacy protection because they usually are not susceptible to interception by the general public. Added to these categories is the new category of "electronic communication." The intention is to provide clarification that there is protection for all forms of electronic communication, including data, even when they may be transmitted by radio.

Section 4 also amends the penalty provisions set forth in 18 U.S.C. 2511(4)(b) by adding language that specifies a similar penalty for intercepting communications "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." The purpose of the amendment is to treat communications using such modulation techniques in the same fashion as those where encryption has been employed to secure communications privacy.

Finally, section 4 amends 18 U.S.C. 2511(2)(a)(i) by clarifying that it is not unlawful for a switchboard operator, officer, employee, or agent of a wire or electronic communication service to intercept, disclose, or use an "electronic communication," in the same fashion as a wire communication, in the normal course of his employment while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of the service. This technical correction is designed to put the handling of electronic and wire communications on the same footing.

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. letter	Webster Hubbell to Leon Panetta re: Digital Telephony Legislation (3 pages)	02/18/1994	P1/b(1)

COLLECTION:

Clinton Presidential Records
Staff Secretary
John Podesta (Subject Files)
OA/Box Number: 17335

FOLDER TITLE:

Digital Telephony [1]

2018-0662-S
rs3150

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]