Amendments to Communications Assistance for Law Enforcement Act (CALEA)

Section-by-Section Analysis

Lawful interception of communications is a critical tool for enforcement of the Nation's laws, protection of its citizens, and maintenance of the national security. Law enforcement agencies at all levels of Federal, State and local government, having the responsibility and the duty to serve these important missions, must ensure that the effectiveness of lawful electronic surveillance is preserved.

However, the complexity and variety of communications technologies and services have dramatically increased in recent years, and the lawful intercept capabilities of the Federal, State and local law enforcement community have been under continual stress, and in many cases have decreased or become impossible. Legal mandates represent a key element of the overall strategy to preserve law enforcement's intercept capabilities in today's world of advancing communications technology. Such mandates, however, must be combined with the continuing efforts of law enforcement agencies to develop and maintain technical electronic surveillance techniques, as well as expanding assistance and cooperation from the many entities that provide communications services. This Bill updates the primary Federal assistance mandate, the Communications Assistance for Law Enforcement Act (CALEA), with a view toward harmonizing such requirements with the other measures necessary to an effective and comprehensive strategy for maintaining lawful interception capabilities.

Congress enacted CALEA in 1994 to help preserve the crucial law enforcement investigative technique of electronic surveillance. CALEA was designed to ensure that Federal, State and local law enforcement would maintain their ability to conduct lawful electronic surveillance in the face of changes in telecommunications technology, regulation, and market forces. The statute largely succeeded in making sure that cellular-telephone carriers -- a nascent industry in 1994 -- would incorporate critical surveillance capabilities into their networks, although implementation difficulties remain with respect to both wireless and traditional land-line telephone services.

Today the world is experiencing a communications revolution, due largely to the Internet. Users can communicate more information faster and to more destinations on the planet than ever before using a single broadband connection. Voice-Over-Internet-Protocol services are also enabling broadband subscribers to replace their traditional telephones. This Bill aims to update CALEA for today's communications revolution by ensuring that it will be understood to apply to the communications services deemed most important for ensuring surveillance access to law enforcement and national security agencies, while at the same time resolving potentially complex issues about the obligations that will be imposed. As discussed herein, such communications services continue to include traditional voice telephony but also the "Voice-

Over-Internet Protocol" services that now provide effective alternatives to traditional services. Such services also include network-access services, such as DSL and cable-modem services. It is critical that law enforcement agencies and those charged with protecting national security maintain a surveillance access point and reasonable surveillance capabilities with respect to rapidly growing network-access services, which enable customers to access a wide array of other communications-related services. In defining the obligations of network-access services, the Bill recognizes that these providers often have little knowledge of the other services that users are accessing through their service.

Another reality of today's communications revolution is that services are being developed and deployed more rapidly and in a more decentralized manner. The Bill therefore reforms the process of creating regulatory safe harbors for CALEA compliance, in order to create incentives for industry associations which develop standards to comply with CALEA's requirements and to lead service providers to build full CALEA compliance into their technologies. It also recognizes the new law enforcement realities and critical national security concerns of the post-9/11 world by strengthening the Act's provisions to provide for efficient and effective enforcement.

The following section-by-section analysis provides an explanation of each amendment in the Bill. For clarity, the section numbers from existing CALEA are retained. The analysis provides the existing law, discusses the purpose for each amendment, and describes the amendment.

Section 102(2) - Amendments to Definition of Call-Identifying Information

The existing definition of the term "call-identifying information" (hereinafter "CII") refers to "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication." It is in some ways akin to addressing and postmarking information on an envelope. Under Section 103(a)(2) of CALEA and under the new Section 103(e), carriers are required to be capable of isolating and enabling the government to acquire this information. The amendments are intended to update the language and remove its ambiguity.

It is important to note that the definition of CII in CALEA and the definitions of "pen register" and "trap and trace" in ECPA, 18 U.S.C. § 3127(3), (4), are not congruent. As the District of Columbia Court of Appeals noted, CALEA "neither cross-references nor incorporates ECPA's definitions of pen registers and trap and trace devices." *See USTA v. FCC*, 227 F.3d 450, 459 (D.C. Cir. 2000). The Court further noted that differences between CALEA and ECPA illustrate the "inherent ambiguity" of the term. Id. Another important distinction is that at least some information that falls within the CII definition is expressly *not* authorized to be acquired from the provider solely with a pen/trap order. In particular, CII has been held to include wireless antenna location information at the origination and termination of a wireless call, but CALEA expressly precludes access to such information from the provider when the government is acting "solely pursuant to the authority for pen registers and trap and trace devices." 47

U.S.C. § 1002(a)(2); *USTA v. FCC*, 227 F.3d at 463 (upholding FCC's decision in the CALEA Third Report and Order that "call identifying information" includes wireless location information).

The "inherent ambiguity" of the CII definition has led to interpretation problems. For example, in 1998 the industry adopted the first CALEA standard, known as J-STD-025. The FBI petitioned for review of the standard to the FCC, contending that it did not provide for the ability to capture all of the necessary aspects of CII, which became known as the "punch list." The "punch list" capabilities, in general, were intended to capture various dialed numbers and signals related to call progress. Much of the ensuing litigation focused on whether any of this information fell within the meaning of the CII definition and, in particular, on the undefined terms "origin, direction, destination or termination." The FCC concluded that many of the "punch list" capabilities were required by CALEA. In a subsequent appeal, the Court of Appeals remanded the FCC's decision, in part based on what the court found to be critical inconsistencies in the FCC's interpretation of these terms. *USTA v. FCC*, 227 F.3d at 460.

The Bill's amendments to the definition of the term "call-identifying information" are intended to: (1) update the language with respect to packet communications; and (2) remove ambiguity created by the terms "origin, direction, destination and termination" by adding additional terms used in ECPA. Additional amendments, including the specification of post-cut-through digits and certain packet-related information within the definition of CII, are discussed further below and are made with regard to other changes included in Section 103, pertaining to a carrier's duty to isolate CII and make it available to the government.

The term "call" is changed to "communication" to make the language less specific to telephony and thereby eliminate doubt about whether CALEA applies to services that are not telephony. The terms "routing" and "addressing" are added to "dialing" and "signaling" for the same reason. This addition mirrors a change to the pen register and trap and trace device definitions in 18 U.S.C. § 3127(3), (4) made by the USA PATRIOT Act. These terms are also inserted throughout CALEA wherever the terms "transmission and switching" now appear, for the same reasons. The phrases "processing" and "transmission" are added to "origin, direction, destination, or termination" in order to remove ambiguities or perceived limitations imposed by the original terms. These additional terms are also intended to ensure that CII encompasses, but is not necessarily limited to, the information available under ECPA's pen register and trap and trace authority, by using terms similar to those used in the USA PATRIOT Act amendments to 18 U.S.C. § 3121(c) ("A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing and signaling information utilized in the processing and transmitting of wire or electronic communications") (emphasis added). The term "or other person" is added to clarify the definition, because the original language appears unintentionally limited to communications of the carrier's "subscriber."

This section is further amended by confirming that it includes (but is not limited to)

certain items of communication-identifying information deemed particularly critical to law enforcement. The first is "post-cut-through digits" which consist of the additional digits dialed after a call is initially set up through the local provider's switch. An example is a 1-800 call to a long distance provider, where the post-cut-through dialed digits are those dialed by the user after the 1-800 call is initially set up. *See USTA v. FCC,* 227 F.3d at 462 ("Some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is 'cut through,' dialing the telephone number of the destination party."). This change is intended to codify current law and to confirm its application to all carriers, including providers of replacement telephone service. Current law requires traditional telephone providers and cell phone providers to maintain the capability to isolate the post-cut-through dialed digits. *See In the Matter of Communications Assistance for Law Enforcement Act,* Order on Remand, 17 FCC Rcd. 6896, 6926-27 ¶ 80 (2002) ("*CALEA Order on Remand*"). The phrase "post-cut-through-digits" is intended to encompass "dialed" and "signaled" and "pulsed" digits, and therefore the phrase "post-cut-through-digits" is employed. This change would not affect the requisite legal authority of the government to obtain post-cut-through-digits.

This section is further amended to specify that communication-identifying information includes (but again is not limited to) certain specified packet-related information, including source and destination Internet protocol and other protocol addresses, the port number, packet file size, and user authentication and logon information, including session time and duration. All of this information is deemed to be within the general definition of communication-identifying information. It is specifically listed herein to avoid potentially lengthy litigation regarding interpretation of the statutory language, because it is critical to law enforcement that carriers implement the capability to isolate this particular information without delay. Again, this change would not affect the requisite legal authority of the government to obtain the specified information.

The following is an illustrative, non-exhaustive list of information that falls within the definition of communication-identifying information:

> called party number; calling party number; start time, end time, call duration; feature invocation and deactivation; feature interaction; registration information; diverted-to number; conference party numbers; post-cut-through dialed digits; in-band and out-of-band signaling; party add, drop and hold information; time, date, size, duration and volume of data transfers; domain names; MAC or Internet Protocol addresses, including both source and destination; port numbers; "to" and "from" information in an electronic mail header; packet sizes; types of protocols or services; special purpose flags; location information; and other header information that meets the definition of communication identifying information.

This list includes information previously determined by the Commission and/or the courts to fall within the existing definition of "call-identifying information." The Bill leaves unchanged the existing requirements with respect to location information. The list also includes additional

information that would derive primarily from the newer services whose coverage is intended to be confirmed through the amendments. While all of this information falls within the meaning of the definition of communication-identifying information, the duty of a carrier to ensure the government's access to such information is governed by Section 103. Under some circumstances defined in that section, a carrier may need only to ensure that the government is afforded access to its customer's packet stream containing the communication-identifying information specified above. Under other circumstances, a carrier may be required to ensure the capability to isolate specific communication-identifying information by extracting it from a packet stream.

Sections 102(6) and 102(10) - Amendments to Coverage Definitions

CALEA's coverage, under current law, is mainly governed by the definitions of the terms "information services" and "telecommunications carrier." The requirements apply to entities that meet the definition of "telecommunications carrier," but exempt them "insofar as they are engaged in providing information services."

The scope of the terms "information services" and "telecommunications carrier" has been difficult to delineate, particularly as newer services combine the characteristics of both, and the formerly distinct telephone and data networks converge. Additionally, both "information service" and "telecommunications carrier" are terms that are used in the Telecommunications Act. *Compare* 47 U.S.C. § 153(20) *with* 47 U.S.C. § 1001(6). Because some communications services that should be covered by the surveillance assistance requirements may be found to be included within the Telecommunications Act's definition of "information services," the similar terms could set unnecessary legal impediments to the proper application of CALEA in these areas.

The amendments are intended primarily to: (1) update the language; (2) preserve CALEA's current applicability; (3) ensure CALEA's application to certain newer technologies, including "replacement telephone service" and "network access service"; and (4) broaden the FCC's authority to deem services subject to CALEA.

A. Section 102(8) - Definition of Telecommunications Carrier

The amendments eliminate the term "telecommunications carrier" and replace it with "communications carrier" in order to remove similarity with the Telecommunications Act, and to confirm the applicability of CALEA's requirements to services without regard to their regulatory status for other purposes. The words "via any technology or method" are also inserted into the general definition of the term found in Section 102(8)(A). This is intended to codify the Commission's prior determinations recognizing that CALEA's requirements are "technology neutral." *See In the Matter of Communications Assistance for Law Enforcement Act,* Second Report and Order, 15 FCC Rcd. 7105 at 7120, n.69 (1999) ("*CALEA Second Report and Order*").

The terms "routing" and "addressing" are added to the existing language of

"transmission and switching" in order to update the language to apply to new communications technologies, including those providing Voice-Over-Internet Protocol services. Similar changes are being made to the definition of "communication-identifying information" in the amendments to Section 102(2), as noted above.

The term "common carrier for hire" in the general definition in Section 102(8)(A) is being retained. This is to ensure that CALEA will continue to cover all entities it currently covers. However, the words "or otherwise on a commercial basis available to the public" are added to ensure that CALEA will apply to any for-hire transmission, switching, routing or addressing service available to the public, notwithstanding whether such service is bundled with another service, offered on a stand-alone basis directly to the public for a fee, or considered a "common carrier" service for other regulatory purposes. The current law requiring resellers of service to ensure CALEA capabilities would remain unchanged. *See CALEA Second Report and Order* at 7120-21, ¶ 24; *CALEA Second Order on Reconsideration*, 16 FCC Rcd. 8959, ¶ 37 (2001) (confirming obligation of resellers to ensure CALEA capabilities). This additional language confirms CALEA's applicability to services offered to the public directly for a fee, or indirectly by being combined with another service. In this regard, the language confirms the inapplicability, for purposes of CALEA, of the Commissions's reasoning in *In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd. 4798, 4823 (2002). In that decision, the Commission opined that cable modem service was not a "telecommunications service" under the Telecommunications Act because it is not made available "for a fee directly to the public." The amendment would not change the Commission's decision, but is intended to limit such decision to interpretations of the Telecommunications Act and to preclude extension of that reasoning to CALEA. Cable modem service, for example, would therefore be covered by CALEA notwithstanding whether it is made available "for a fee directly to the public," or whether providers thereof are considered "common carriers" for other regulatory purposes. Likewise, the amendments will confirm CALEA's applicability to other communications services, notwithstanding the technology used. Under the existing law, some confusion has existed with regard to services such as the so-called "short message service" and "push-to-talk" service, largely based on the newer technology used to provide such services. See *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd. 15,676, 15725 ¶ 144 (2004) (holding CALEA applicable to push-to-talk services). The amendments will confirm the coverage of push-to-talk, short message service, voice mail service, and other communications services offered on a commercial basis to the public are covered.

Subsection 102(8)(B) is amended to include an illustrative, non-exhaustive, list of types of carriers subject to CALEA. Subsection (B)(i) retains existing language applying CALEA to providers of "commercial mobile service." New subsections (B)(ii) and (iii) contain newly defined terms "network access service" and "replacement telephone service." These terms are defined in new Sections 102(9), (10). These terms are intended to confirm CALEA's application to providers of broadband Internet access, and certain types of "Voice-Over-Internet-Protocol" (VOIP) (not including certain applications that solely provide the ability to obtain addressing

from other users). These new terms are also used to define new capabilities required for certain network access service carriers under Section 103.

Subsection 102(8)(B)(iv) (formerly (B)(ii)) is amended to broaden the FCC's authority to deem an entity subject to CALEA "to the extent that the Commission finds that it is in the public interest." The amendments include removing the requirement for a finding that the entity is engaged in a service that is a "replacement for a substantial portion of the local telephone exchange," which is potentially too limiting. The Bill also adds a section providing that, in determining the "public interest," the Commission will consult with the Attorney General, in order to ensure that the Commission obtains his assessment of the needs of law enforcement, public safety or national security. This is appropriate because the Department of Justice is in the best position to assess such needs. As discussed below, it is also intended that the FCC will be able to exempt a service from the "exempt services" section by using this authority.

Due to the constant change of the technology, a comprehensive list of covered carriers is neither possible nor desirable, however the following provides an illustrative non-exhaustive list of carriers intended to be covered by these amendments: Voice-Over-Internet-Protocol providers, subject to the exemptions discussed below; broadband Internet Access providers, including providers of facilities-based access using DSL, cable modem or other wired technologies, broadband over powerline, radio, satellite, electromagnetic, photooptical or photoelectronic facilities. Again, this list is not intended to be all-inclusive.

Subsection 102(8)(C) retains the concept that a communications carrier "does not include persons or entities insofar as they are engaged in providing" exempt services. However, the amendments to subsection 102(6)(C)(iii) provide that the term "exempt services" does not include any service subject to a determination by the Commission under subsection (8)(B)(iv). This provision authorizes the Commission to override the exempt services clause by making a determination under its authority contained in subsection 102(8)(B)(iv). Similar language has been inserted into subsection 103(b)(2), which currently exempts from CALEA's assistance capability requirements any "information services," "private networks," and equipment that is for the sole purpose of "interconnecting" carriers.

B. Section 102(6) - Definition of Information Services

This provision is amended to eliminate both the term and the definition for "information service." This change is intended to eliminate similarities with the Telecommunications Act, and confirm that CALEA may apply to a service or entity that is otherwise exempted from regulation under such Act. It is also intended to limit all CALEA exceptions to only those services and applications that are "accessed" through an already-covered service (e.g. network access service). The intent here is to ensure that an interception capability will be maintained with respect to communications transmitted to or from an exempt service. For example, the service used to transmit an electronic message (e-mail) would be covered, but the service used to store

or process the electronic message would be exempt. CALEA's original legislative history suggests that this was Congress's original intent:

> "[T]he capability requirements only apply to those services or facilities that enable the subscriber to make, receive or direct calls. They do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America-on-Line or Mead Data, or Internet service providers. (The storage of a message in a voice mail or E-mail 'box' is not covered by the bill. The redirection of the voice mail message to the 'box' and the transmission of an E-mail message to an enhanced service provider that maintains the E-mail service are covered.)"
>
> H.R. Rep. 103-827, pt I, at 23 (1994).

As discussed below, the amendments likewise cover transmission services even where bundled or combined with an otherwise exempt service.

Subsections (A)(i) through (A)(v) describe the types of "exempt services" under CALEA. It is intended to exempt certain general types of services reached via a public network, such as the Internet, but not exempt the transmission path by which the network is reached, such as via a network access provider.

Subsection (i) retains the term "processing" from the original definition of "information services." This section is intended to exempt remote computer processing.

Subsection (ii) clarifies that the exemption originally found in Section 102(6)(B)(i) applies to storage and retrieval "facilities." It is intended to exempt computer servers, such as those accessed when web browsing, to the extent that they provide only storage and retrieval facilities. The Bill is intended to be interpreted such that so-called "Internet Service Providers" (ISPs) would only be covered to the extent they combine their services with or resell the transmission service used to reach the end-user. ISPs today are significantly different entities from those that Congress intended to exempt from CALEA in its original enactment. In 1994, public access to the Internet was generally afforded through the services of an ISP reached via a "dial-up" connection provided by a common carrier. Entities today often combine both aspects, and utilize "broadband" rather than dial-up facilities. Cable modem service is one example, discussed below. The intent of these amendments, as discussed below, is to maintain the applicability of CALEA to the transmission portion of the service, notwithstanding that it may be combined with other information processing or storage and retrieval services that may be deemed exempt.

Subsection (iii) retains the "electronic publishing" exemption in the original statute (formerly Section 102(6)(b)(ii)).

Subsection (iv) is a new definition that is intended to exempt the provision of a software

application that solely permits the retrieval from other users of addressing information, without any other assistance (including provision of a directory service) from the provider of the application. It is intended that law enforcement access to communications associated with such applications would occur through the carrier supplying a network access service to the user. Specifically, the definition exempts certain software-based applications that solely enable a user to obtain addressing or routing information from other users. It is not intended to exempt the provider of a software-based application when such provider also offers any routing, transmission, addressing or switching or other service or assistance, including offering a computer server that provides a directory or look-up service.

Subsection (v) retains the existing exemption for "electronic messaging services." No court has yet interpreted the definition of "electronic messaging services." Congress intended in the original enactment that this term would apply to certain forms of electronic mail service, as stated in CALEA's legislative history:

> "The term 'information services' includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (including but not limited to multimedia software) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, Microsoft Mail, Microsoft Exchange Server, and AT&T Easylink (and their associated services) are both examples and precursors.
> ***
> By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill."
>
> H.R. Rep. 103-827, pt I, at 21(1994).

An electronic messaging service is therefore a separate service that is accessed via another transmission service that is covered by CALEA. An example is a web-based electronic mail provider that is accessed through a covered network access service carrier. It is intended that the interception access point for these types of electronic mail services would be at the network access service provider.

Subsection 102(6)(B) is intended to exempt those who are not otherwise communications carriers when they share a network access service with their patrons on or near their premises. For instance, a retail business that incidentally provides wireless Internet connections on its premises will be exempt if the service the business allows its patrons to share complies with the requirements of section 103. In the case that either (1) a business or other entity already has an existing contract in force for the service being shared or (2) no service that complies with section 103 is available to the business or other entity, the obligation to share only a compliant service is relieved. A business or other entity that has a contract for non-compliant service will no longer be permitted to share a non-compliant service after the expiration of that contract, unless no

compliant service is available. The limitation that the service must be intended to provide access within 300 feet of the premises realizes that businesses may choose to use technologies such as wireless access points that allow access just beyond their premises and that circumstances such as power fluctuations or non-standard user configurations could cause signals to exceed 300 feet. Notwithstanding such unintended possibilities, the service would remain exempt so long as the equipment used by the sharing entity was intended by the sharing entity to provide service within 300 feet of its premises.

Subsection 102(6)(C) is amended to address the situation where an exempt service (e.g. electronic messaging service) and a covered service (e.g. network access service) are combined and alleged to become a single integrated service. The intent is to maintain CALEA's applicability with respect to the covered portion of the service notwithstanding a combination or "bundling" of two types of service. The necessity for ensuring this point is illustrated in the FCC's approach to cable modem service, which the FCC concluded was a combination of "telecommunications" and "data processing" that is "a single [information] service" under the Telecommunications Act. *In re: Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities*, FCC 02-77 (March 15, 2002), ¶ 39 (holding that cable modem service is an "information service" under the Telecommunications Act because the "telecommunications component [of cable modem service] is not, however, separable from the data-processing capabilities of the service. As provided to the end-user the telecommunications is part and parcel of the cable modem service and is integral to its other capabilities."). The amendments make it clear that, for purposes of CALEA, the communications component of a bundled service would be subject to CALEA.

As discussed above, the changes to subsection (C) are also intended clearly to permit the FCC to *remove* a service from the exemption (and thus bring it within CALEA's ambit) by using the authority in subsection 8(B)(iv).

C. Sections 102(9) and (10) - New Carrier Definitions

The new definition in Section 102(9) for "network access service" confirms CALEA's application to what is commonly referred to as "broadband Internet access." It is intended to cover DSL, cable modem, and any other methods of network access. The definition is intended to cover transmission services, as distinct from the variety of services that can be provided *via* the network access service. For example, the definition does not include "VOIP" telephony, which falls within the definition of "replacement telephone service."

The new definition in Section 102(10) for "replacement telephone service" confirms CALEA's application to certain types of service commonly referred to as "VOIP." This definition *excludes* providers of certain software applications that only enable a user to obtain information from another user. In general, it is intended to cover those services where a carrier is providing or managing the transmission, switching, routing or addressing, including providing a directory to supply such addressing, but not applications that solely enable a user to obtain the addressing information from another user.

## Section 103 - Amendments to Assistance Capability Requirements

Section 103 of the existing CALEA sets forth the surveillance assistance capabilities required for all telecommunications carriers. This Section provides for four carrier duties, which are generally summarized as follows: (1) isolate and ensure the capability to intercept communications; (2) isolate and ensure the capability to acquire call-identifying information that is "reasonably available" to the carrier; (3) provide for the delivery of intercepted communications and CII via government procured facilities; (4) facilitate interceptions in a manner that ensures privacy of communications not authorized to be intercepted and information regarding the government's interception.

The amendments fall into two general categories. First, several amendments are intended to clarify certain aspects of the requirements described above. Second, a new Section 103(e) is being added for the purpose of modifying such requirements for providers of network access service.

### A. Section 103(a)(1)-(2), 103(g) - Domestic Point of Presence for Surveillance

Amendments to subsections 103(a)(1) and (a)(2) add a requirement for each carrier to maintain a point of presence within the United States at which interception or access to communication-identifying information can be performed. The purpose of this requirement is to address situations where carrier equipment is located in a foreign country, thereby making law enforcement access difficult and less secure. An example of this is found in the case of satellite service providers who maintain earth-station gateways in a foreign country. The requirement established by the amendment would require such providers to establish earth-station gateways in the United States, but such requirement would, under new subsection 103(g), be subject to waiver by the Attorney General under mutually agreed conditions. This provision recognizes that the requirement might, under circumstances agreed by the Attorney General, be met through other means. The establishment of a network switch or other network point-of-presence within the United States at which communications and communication-identifying information could be lawfully intercepted or accessed is one possible example.

### B. Section 103(a)(2) - Clarify the Scope of Communication-Identifying Information that Carriers Must Isolate

Section 103(a)(2) is further amended by including the phrase “used by the carrier in the transmission, routing, addressing or switching of wire or electronic communications or, if not used by the carrier, is otherwise [reasonably available].” The additional language is intended to supplement the term "reasonably available" and to provide that carriers must isolate and provide to the government any communication-identifying information that they use in the transmission, switching, routing or addressing of communications.

The term "reasonably available" has been the source of interpretational difficulties in

industry standards-forming groups and has generated litigation. The "punch list" litigation revolved around this term, among other issues, since the industry argued that each disputed capability was not "reasonably available." The FCC ultimately adopted a definition of the phrase, finding that "call-identifying information is 'reasonably available' to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications." *In the Matter of Communications Assistance for Law Enforcement Act,* Third Report and Order, 14 FCC Rcd. 16794, 16802-03 ¶ 14 (1999); 47 C.F.R. § 22.1102; *In the Matter of Communications Assistance for Law Enforcement Act,* Order on Remand, 17 FCC Rcd. 6896, 6926-27 ¶ 80 (2002) ("*CALEA Order on Remand*") ("We think . . . something is 'available' if it is accessible . . . . [I]f information is only accessible by significantly modifying a network, then we do not think it is 'reasonably' available."). The FCC's definition, however, may only continue disputes as to the scope of "reasonably available" information, because it turns on another undefined concept: "significant network modification."

This amendment is intended to clarify the scope of communication-identifying information that a carrier is obligated to isolate and to enable the government to acquire so that it includes, at a *minimum*, the information that the carrier uses in the processing and transmitting of wire or electronic communications. Since several of the original "punch list" items included signals actually used by the carrier (e.g. subject signaling; network signaling; party hold, drop, join messages; location information), this clarification could reduce litigation, as it would ensure that carriers are clearly obligated to ensure law enforcement access to such information. The amended subsection retains the original phrase "reasonably available" in order to preserve the FCC's decisions regarding communication-identifying information that is not used by the carrier in processing communications but is nevertheless available to the carrier. For example, the FCC determined that "post-cut-through dialed digits" are reasonably available with respect to certain carriers, even though such digits may not be used by such carriers. *CALEA Order on Remand*, at 6826-27 ¶ 80.

C. Section 103(a)(3), (f) - Amendments to Delivery Requirements

Existing law under Section 103(a)(3) requires carriers to ensure that intercepted communications and CII are delivered to the government 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." The amendment inserts the phrase "standard, commercially available, and reliable" to further describe the format in which carriers are to provide for delivery of such communications and CII. It is intended to require carriers to deliver intercepted communications in a standard format or protocol, rather than in a proprietary, non-standard, or unreliable format or protocol.

An additional new requirement, specified in new subsection 103(f), would authorize the Commission to specify by rule one or more standard, commercially available, reliable delivery formats to be used by a particular class or category of communications carriers. Such rules could also be made applicable to particular services of a communications carrier, as deemed appropriate by the Commission. This rulemaking authority extends also to the delivery and

storage requirements for network access carriers described below with regard to new section 103(e).

D. Section 103(a)(4) - Duty to Ensure Privacy and Interception Security

Existing law under Section 103(a)(4) requires carriers to facilitate interceptions (and access to CII) "unobtrusively and with a minimum of interference with any subscriber's telecommunications service" and "in a manner that protects the privacy and security of communications not authorized to be intercepted and information regarding the government's interception of communications and access to CII."

The amendment clarifies these requirements by adding additional language providing that they should not be interpreted to *preclude* any interception or access to communication-identifying information. The purpose of the amendment is to make clear that the carrier's duty in this regard does not override its primary duty to facilitate access to all of the communications or communication-identifying information that a law enforcement agency has been authorized to obtain. The carrier's privacy duty is clarified by adding a proviso that is intended to confirm that such requirements would not preclude a carrier from affording the government access to a subject's full packet stream and using a process to extract a more limited set of information. Additional provisions discussed below are intended to require network access providers to isolate a subject's full packet stream.

E. Section 103(c) - Amendments to Carrier-Premises Monitoring

Subsection 103(c) currently authorizes a carrier to comply with the delivery requirement of Section 103(a)(3) by allowing a law enforcement officer to conduct monitoring at the carrier's premises in the carrier's discretion and under certain circumstances. The amendment clarifies that allowing such monitoring in a carrier's discretion need not be under circumstances where that is the "only" means of accomplishing the interception. The amendment also recognizes that the carrier must allow such monitoring if required to by a lawful order or other authorization.

F. Section 103(e) - Network Access Service Assistance Capability Requirements

New subsection 103(e) and related changes to section 102(2) are intended to clarify the assistance capability requirements specified in CALEA for "network access service" providers (e.g. broadband Internet access providers). Network access service providers are to ensure the following capabilities: (1) isolate a customer's or user's packet stream; (2) isolate the communication-identifying information used by the carrier, plus other reasonably available communication-identifying information (pursuant to subsection 103(a)(2)); (3) store the isolated packet stream or the set of isolated communication-identifying information if requested and under conditions specified by the law enforcement agency conducting surveillance; and (4) enable the delivery of the isolated packet stream or isolated communication-identifying information to a facility specified by the law enforcement agency conducting surveillance for recording or further processing to extract the authorized information. The same requirements for

a point-of-presence within the United States found in subsections 103(a)(1), and (2), and 103(g) are also required here.

The need for further clarity here lies in the nature of packet-switched networks. Packetized communications may contain a variety of addressing, routing and related information and convey a variety of services. Much of this information merely passes through a network access carrier's system without being "read" or otherwise detected by the network equipment, because the information is contained in a different "layer" and may be formatted using a different protocol from the one the carrier's network uses to transmit communications. E-mail to/from addresses are an example in some situations. Isolating this type of pass-through information requires extracting it from packets using specialized filtering devices or other processes. A commercial example of such an extraction capability is "Etherpeek."

Extraction of communication-identifying information for specific services not provided by the communications carrier is considered costly and technically difficult by the industry. The amendments address industry concerns by continuing to impose the existing legal standard upon network access carriers that they isolate only "reasonably available" information, which under the modified version of section 103(a)(2), would include (but not be limited to) the information a carrier "uses" to route information. This is a requirement that a carrier should be able to meet without undue burden. This provision further requires a network access carrier to isolate the subject's entire packet stream. These amendments would not require such carriers to maintain the ability to extract particular types of packet streams (communications services) or other communication-identifying information carried within the packet stream that are not otherwise "reasonably available." It is not feasible to require network access carriers to maintain full extraction capabilities for services they do not control in a manner that is sufficiently accurate, reliable and up-to-date to properly meet the needs of law enforcement agencies. Additionally law enforcement agencies have obtained, or given additional resources could obtain, the technology (filtration techniques) to extract the authorized communications or communication-identifying information from the isolated packet stream. The development of such capabilities requires an ongoing maintenance and engineering research effort, because new communications protocols and technologies are constantly added to the marketplace. Hence appropriate resources will need to be allocated for this purpose.

The technology associated with law enforcement filtration techniques often requires regulation of the total flow of data through the law enforcement device. In order to keep this flow within manageable limits, some temporary storage or buffering may be necessary. Typically, it will be necessary for the carrier to maintain this type of storage for no longer than a few hours before the buffer is emptied. For this reason, proposed section 103(e)(3) requires network access service carriers to be capable of storing communications and other information for a time period specified by the law enforcement agency as necessary to effectuate the interception or access. The provision does not expand nor limit any existing legal authority, under 18 U.S.C. § 2703(f) for example, for a law enforcement agency to require an entity to retain records.

## Section 104 - Amendments to Capacity Requirements

CALEA requires carriers to provide for the capability to accommodate multiple simultaneous interceptions, pen registers, and trap and trace orders. The level of the capacity requirement is to be specified in a Notice issued by the Attorney General. *See, e.g.*, FBI Final Notice of Capacity, 63 Fed. Reg. 12218 (1998). The Notice also triggers a carrier's duty to comply with the capacity requirements. Since CALEA's enactment, carriers' systems have developed such that they usually are not limited in terms of the number of wiretaps, pen registers and trap and trace orders that they are able to accommodate at the same time. For example, the FBI-developed "dial-out solution," which permits intercepted communications to be delivered to a law enforcement agency via an ordinary telephone line, renders interception capacity largely a moot issue.

Since issuance of further notices of capacity may be unnecessary for law enforcement, the changes to Section 104(a) and (c), and the addition of a "minimum capacity" requirement of two simultaneous interceptions, pen registers and trap and trace orders for each of a carrier's switching, addressing, routing, or transmission facilities, is intended to make further capacity notices discretionary.

## Sections 105 and 229 - Amendments to System Security and Integrity Requirements and Commission Investigation and Enforcement Requirements

CALEA's existing system security and integrity provision, Section 105, requires that interceptions within a carrier's switching premises be activated only in accordance with a court order or other lawful authorization and with the affirmative action of a carrier employee acting in accordance with Commission regulations. The Commission has adopted rules under this provision pursuant to its authority in CALEA Section 229(b). *See* 47 C.F.R. § 64.2100-.2106.

The amendments add to Section 105 a requirement that the carrier employee activating the interception must be "within the United States." This amendment addresses the increasingly common situations involving foreign-located carrier equipment or employees, and is consistent with the changes to Section 103 requiring a surveillance "point-of-presence within the United States." The amendment also mandates FCC adoption of rules under Section 229(b) directed toward surveillance security, including: (1) a 24/7 point-of-contact for law enforcement; (2) disclosure of the names and other identifiers for employees or other persons under a carrier's control upon law enforcement request; and (3) location of surveillance-assistance employees within the United States. The first requirement is a codification of an existing FCC rule applicable to common carriers. *See* 18 U.S.C. § 64.2103(b)(4). The amendments will ensure application of such requirement to other carriers subject to CALEA, including but not limited to network access service providers and replacement telephone service providers. The second requirement is intended to provide a mechanism for enhancing the security of communications interceptions, by providing law enforcement agencies with an ability, if they deem it necessary to acquire information, regarding the backgrounds of carrier personnel involved with facilitating surveillance. This is intended to provide law enforcement agencies with minimal background

information, while at the same time recognizing that requiring all carriers to conduct background investigations could impose an undue burden. The final requirement is addressed at providing further security for situations where a carrier maintains foreign-located facilities.

The changes to Section 229(c) and (d) of the Communications Act of 1934 are intended to provide the FCC with the authority and mandate to enforce provisions of CALEA. The amendment clarifies the existing requirement found in Section 229(c) for the Commission to "conduct such investigations as may be necessary to insure compliance by common carriers with the requirements of the regulations prescribed under this section." This authority would be in addition to the judicial authority, as described in Section 108 below.

Section 106 - Cooperation Between Manufacturers and Carriers

The bill does not change Section 106 except to add “routing” and “addressing” to the existing “transmission” and “switching.”

Section 107 - Safe Harbor Standards and Commission Rulemaking Authority

Existing law in Section 107(a) of CALEA provides a carrier with a "safe harbor" for compliance with the requirements of Section 103, if it is in compliance with "technical requirements or standards" adopted by an industry association or standard-setting organization. Standards are engineering specifications and are often relied upon in the communications industry to establish interoperable systems. They are formed by committees comprised of representatives from various companies within the industry. Standards formed to meet CALEA requirements have legal significance in that, once adopted, the standards provide a "safe harbor" for a carrier's compliance with the assistance capability requirements.

Existing law under Section 107(b) provides a process by which the government, or other person, can petition the FCC for a determination that a standard is deficient. The Commission is authorized to establish by rule technical requirements or standards that meet four criteria specified in Section 107(b)(1) through (4), including: (1) meet the assistance capability requirements by cost effective methods; (2) protect privacy; (3) minimize the costs to residential ratepayers; and (4) encourage the provision of new technologies. The Commission may also provide a reasonable time and conditions for compliance with the new standard.

Although compliance with a standard is not mandated by CALEA, it is generally considered by the industry to be the preferred method of compliance because it is the only way to achieve the desirable assurance of a safe harbor. Two primary concerns are associated with the safe harbor provisions. First, the set of capabilities contained in an industry-adopted standard may be inadequate. Law enforcement's only recourse under current law is a time-consuming petition to the FCC; meanwhile, the industry-adopted standard is a safe harbor until the FCC says otherwise. This was the case with adoption of the J-STD-025, and the FBI’s subsequent petition to the FCC to require the "punch list" capabilities. Second, industry associations in some cases delay the adoption of any standard at all, which can delay the

development of surveillance solutions.

The amendments address these issues by (1) providing that, in the event that the AG files a petition for deficiency with regard to an industry-adopted standard, such standard would not become a safe harbor until approved or otherwise modified by the FCC; (2) ensuring the existence of a mechanism for the Attorney General to propose a standard which would become a safe-harbor after approval by the FCC, and to petition the FCC to adopt rules to satisfy Section 103 and determine coverage; (3) clarifying the criteria under which the FCC is to adopt such rules.

Currently even a deficient standard would arguably become a safe harbor immediately upon adoption by an industry organization, and remain so during the pendency of what could be a lengthy FCC proceeding. The amendments to Section 107(b) will preclude that occurrence when the AG seeks FCC review of a standard, until such time as the Commission either approves the standard or modifies it by adopting necessary rules. An industry-adopted standard will continue to accord safe-harbor status, as under current law, when the AG does not file a petition for FCC review of whether the standard is in compliance with the assistance capability requirements.

The revised Section 107(b) (now Section 107(b)(1)) makes clear that the FCC has authority to determine coverage and adopt rules to say what Section 103 requires as to a given service. The FCC could use this authority, among other things, to approve Attorney General-adopted standards, to approve or modify industry-adopted standards, or to adopt rules itself, for example, to declare that a particular technical capability is required by Section 103. The FCC would be obligated to respond to a petition (whether filed by industry or the Attorney General) within 180 days, but the Attorney General could further expedite such decision by certifying that emergency conditions exist. Section 107(b)(1)(C)(i)-(iv) retains, in amended form, the four criteria specified in existing Section 107(b)(1) through (4). However, the amendments provide that the Commission's rules must first "meet the assistance-capability requirements of Section 103" and, subject to meeting those requirements, should promote the use of methods that satisfy the four criteria, including cost-savings. The intent of this amendment is to ensure that the Commission's rules will first and foremost ensure the surveillance capability requirements, and that the other criteria will be satisfied through a consideration of alternative methods of meeting such requirements.

The provision in Section 107(b)(3) would also require the FCC to consult with the Attorney General as to the needs of law enforcement, public safety, and national security. This is warranted because the Attorney General is best suited to making such judgements. The Attorney General's analysis will likely continue to be provided to the industry through the publication of surveillance "needs documents," as is the FBI's current practice.

Section 107(c) currently gives the FCC authority to provide extensions to carriers who deploy or proposed to deploy equipment before "the effective date of Section 103." The effective date of Section 103 was 4 years after enactment of CALEA in 1998. The FCC has

tentatively concluded that this provision applies only to pre-October 25, 1998 equipment. *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd. 15,676, 15725 ¶ 97 (2004). The changes to this Section would bar any further extensions for pre-1998 equipment beyond a date certain – set at one year after [the day before the bill is introduced], and requires a precise factual showing for any carrier still seeking an extension under this Section.

Section 108 - Amendments to Provisions Concerning Enforcement Orders

Section 108 of the current statute requires a court to find, before issuing an enforcement order, 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 CALEA 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. This Bill revises each of those two criteria.

The amendments would allow consideration of the availability of alternative technologies only under Section 2522(a), in cases where a court has issued a surveillance order. The provision would allow a communications carrier to be found in compliance where alternative technologies or the facilities of another carrier are reasonably available to the law enforcement agency or officer seeking enforcement for the expeditious implementation of the authorized surveillance. The availability of such alternative technologies or facilities would not, however, be a defense to an action brought by the Attorney General under 18 U.S.C. § 2522(b), seeking an order directing that a communications carrier, a manufacturer of communications transmission or switching equipment or a provider of communications support services comply with CALEA.

The amendments would eliminate the provision in Section 108(a)(2) requiring that a court find that compliance with CALEA's requirements is reasonably achievable. The current provision could be interpreted as placing a burden of proof on the government to demonstrate that compliance is reasonably achievable in each enforcement action. The amendments are premised upon the fact that the statute's requirements are designed to be reasonable, and that Section 109(b) provides a mechanism for anyone subject to its provisions to seek relief in the event that compliance is not reasonably achievable. A finding by the Federal Communications Commission pursuant to Section 109(b) that compliance is not reasonably achievable would remain a defense to an enforcement action pursuant to Section 108(c)(2). This amendment would also ensure that highly technical questions of reasonable achievability are decided by the Commission rather than by a court.

The Bill also amends Section 108(c)(3) to eliminate uncertainty regarding the meaning of "significantly upgraded" and, consistent with amendments to Section 109, to eliminate the exemption for pre-1995 equipment and facilities as of January 1, 2008.

Section 109 - Amendments to Provisions Concerning Payment of Costs

The new Section 109(b)(1) makes clear that communications carriers are responsible for payment of all costs directly associated with any modifications they may need to perform in connection with equipment, facilities or services installed or deployed after January 1, 1995, to establish the capabilities necessary to comply with Section 103. The new Section 109(f) makes clear that a communications carrier is not permitted to include the costs of complying with this Act in any charges to any government agency or officer that such a carrier may submit to the government to cover its costs of complying with a particular surveillance order.

The amendments to Section 109(b)(1) (redesignated as Section 109(b)(2)) should help ensure that any petition to the Commission seeking a determination that compliance with this Act's requirements is not reasonably achievable must include a detailed description and supporting documentation setting forth the technical modifications and related costs necessary to achieving compliance with respect to each service and requirement from which relief is sought. The amendments also make clear that the burden is on the communications carrier to show that relief is warranted. In order to reflect the importance of these determinations to both the industry and law enforcement, the Bill shortens the period for Commission action on the petition from the 1 year provided in the original enactment to 180 days. The additional changes to Section 109(b)(2) (redesignated as Section 109(b)(3)) provide that any FCC finding that compliance is not reasonably achievable shall permit an exemption from Section 103's capability requirements for no longer than a period of two years, provided that the Attorney General may seek reconsideration at any time. Reconsideration is likely to be sought under circumstances of urgency; hence the Commission's decision is required to be made within 90 days.

Section 109(d) of the current statute provides that pre-1995 equipment need not be brought into compliance with Section 103's assistance-capability requirements unless the Attorney General agrees to pay the costs of such an upgrade or until such time as the equipment "is replaced or significantly upgraded" or "undergoes major modification." This Bill eliminates the "significantly upgraded" and "major modification" provisions, which have proven difficult to apply, and sets a firm cutoff date of January 1, 2008, after which this exception will no longer be available to such carriers.

Amendments to Title 18, United States Code

Section 2522 of Title 18, United States Code, provides for enforcement of CALEA's provisions. This Bill makes technical amendments to Section 2522(a) to make explicit that enforcement of CALEA is available in contexts where a court has authorized a pen register or trap and trace device under the Foreign Intelligence Surveillance Act of 1978.

The Bill also adds language to Section 2522(a), Section 2518(4), and Section 3124(f) to clarify that assistance to law enforcement required by CALEA is in addition to, and not a substitute for, the general assistance duty required of any person pursuant to an order issued under Title III of the Omnibus Crime Control and Safe Streets Act (18 U.S.C. § 2510, et seq.) or

the Pen/Trap Statute (18 U.S.C. § 3121, et seq.).

The Bill further amends Sections 2518(4) and Section 3124(c) to require that any expenses for which a communications carrier seeks reimbursement from law enforcement be itemized. This change helps implement the clarifications to Section 109 that ensure that a communications carrier is responsible for, and may not charge the government for, the costs of bringing its equipment into compliance with CALEA.

Section [X.1] sets forth an anti-liability provision for CALEA compliance that is similar to and based on the language that is currently found in Title III and the Pen/Trap Statute at 18 U.S.C. §§ 2511(2)(a)(ii), 3124(d). The new CALEA-specific language may be added to CALEA, or the provision may be incorporated into the cited sections of Title III and the Pen/Trap Statute. The amendment would provide carriers with further assurances that compliance with any provision of CALEA could not subject the carrier to civil liability. Carriers have at times argued that implementing surveillance capabilities could subject them to liability. This amendment could therefore promote compliance.

Amendments to the Communications Act of 1934

Section 229 of the Communications Act of 1934 [47 U.S.C. § 229] requires the Commission to make rules to implement CALEA generally, and specifically to require carriers to establish policies and procedures to protect the security and integrity of their systems, and to conduct investigations as to CALEA compliance. Most of the amendments to Section 229 are explained above with regard to Section 105.

The Bill further adds a new subsection (g) to Section 229 to require the Commission to inquire into and consider a carrier's non-compliance with CALEA and to consider such non-compliance to be a factor weighing against any determination that any relief sought by such carrier under the Communications Act is in the public interest.