

# **THE BALLER HERBST LAW GROUP**

A PROFESSIONAL CORPORATION

2014 P STREET, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 833-5300

FAX: (202) 833-1180

[www.baller.com](http://www.baller.com)

JAMES BALLER  
TELEPHONE: (202) 833-1144  
PORTABLE: (202) 441-3663  
INTERNET: [Jim@Baller.com](mailto:Jim@Baller.com)

MINNEAPOLIS OFFICE  
377N GRAIN EXCHANGE BUILDING  
301 FOURTH STREET SOUTH  
MINNEAPOLIS, MN 55415-1413  
(612) 339-2026

January 12, 2007

## **The Communications Assistance for Law Enforcement Act (CALEA): Key Legal and Technical Requirements and Options**

**The Baller Herbst Law Group  
and  
Columbia Telecommunications Corporation**

### **I. INTRODUCTION**

The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires providers of telecommunications services, Internet access services, or certain kinds of Voice over Internet Protocol (VoIP) to acquire technical capabilities that will enable them to assist law enforcement officials in conducting authorized interceptions of communications content or call-identifying information.

**All communications providers covered by CALEA, *without exception*, must become CALEA-compliant by May 14, 2007, and must file interim reports by February 12 and March 12 to show that they are diligently pursuing ways to comply with CALEA. The Federal Communications Commission (FCC) has stated that it will not grant extensions of time. Parties that fail to meet their CALEA obligations are subject to fines and civil penalties of up to \$10,000 for each day in violation.**

As shown below, complying with CALEA is likely to be extremely expensive and burdensome. For example, an affected provider with 15,000 subscribers could be subject to up-front capital costs in the range of \$100,000 and to ongoing expenses of several thousand dollars a month. As a result, numerous affected parties have challenged these requirements at the FCC, in the courts, and before Congress. All such challenges have failed, and potentially affected parties must now promptly determine whether and how CALEA affects them and what technical and legal options they may have.

In this document, Baller Herbst and Columbia Telecommunications have joined together to provide potentially affected parties an overview of the history and purposes of CALEA, the entities that it covers, the obligations that it imposes, and the main technical and legal options that are available to them. In particular, we discuss a process through which some providers, after studying their options diligently and finding that none is “reasonably achievable,” may be able to shift some or all of their CALEA compliance costs to the U.S. Department of Justice (DOJ).

## II. WHAT DOES CALEA DO?

CALEA<sup>1</sup> was enacted in 1994 at the behest of the DOJ. Its purposes of CALEA are succinctly summarized in House Report accompanying the Act.<sup>2</sup> These are

to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, ... while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services. To [e]nsure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability to:

- (1) isolate expeditiously the content of targeted communications transmitted by the carrier within the carrier's service area;
- (2) isolate expeditiously information identifying the origin and destination of targeted communications;
- (3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and
- (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications.

Of particular relevance here are the "assistance capability requirements" set forth in Section 103 of the Act. Section 103 does not affect the scope of the government's surveillance powers. Rather, it imposes legal requirements on "telecommunications carriers" (defined below) to implement technical capabilities and changes necessary to meet the evolving needs of law enforcement.

Section 103 is performance-based in that it authorizes covered parties to adopt any approach that will enable them to comply with the mandates of Section 103. CALEA and the FCC have, however, sought to encourage providers to adopt approaches that are consistent with emerging industry standards applicable to CALEA. Specifically, the Telecommunications Industry Association has adopted and published standards collectively designated "J-STD-025" and known colloquially as the "J-Standard." These standards outline in detail the technical features, specifications and protocols for affected providers to use in making subscriber communications and call-identifying information available to law enforcement agencies having appropriate legal authorization. These standards are not exclusive, however, nor will they necessarily work for all affected providers.

---

<sup>1</sup> Pub. L. No. 103-414, 108 Stat. 4279.

<sup>2</sup> House Report No. 103-827, 103d Cong., 2d Sess. 9 (1994).

### **III. WHO IS SUBJECT TO CALEA?**

#### **A. “Telecommunications carriers”**

On its face, CALEA applies to “telecommunications carriers” and exempts providers of “information services.” For the purposes of CALEA, however, these terms do not have the same meanings as they do in other federal communications laws. Under CALEA, a “telecommunications carrier” is not merely a provider of traditional circuit-switched telephony services, but also a provider of “facilities-based broadband” and “interconnected VoIP” services.<sup>3</sup>

##### **1. “Facilities-based broadband services”**

The FCC has defined providers of “facilities-based broadband services” as including “entities that provide transmission or switching over their own facilities between the end user and the Internet Service Provider.”<sup>4</sup> This broad definition includes all entities that provide broadband services over their own facilities or over unbundled network elements (including leased lines and wireless channels) obtained from incumbent local exchange carriers.<sup>5</sup> Unless they meet the “private network” exception described below, providers that offer FTTP broadband, cable modem, or DSL service are all subject to CALEA.<sup>6</sup> The same logic would also apply to providers of wireless Internet access services.

##### **2. “Interconnected VoIP”**

The FCC has also concluded that CALEA applies to providers of “interconnected VoIP services,” which it has defined as follows for the purposes of CALEA:

[I]nterconnected VoIP services include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user’s location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from *and* terminate calls to the PSTN... To be clear, a service offering is ‘interconnected VoIP’ if it offers the *capability* for users to receive calls from and terminate calls to the PSTN; the offering is covered by CALEA for all VoIP communications, even those that do not involve the PSTN. Furthermore, the offering is

---

<sup>3</sup> Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, *First Report and Order and Further Notice of Proposed Rulemaking*, 20 FCC Rcd 14989, 15001-12 ¶¶24-40, rel. August 5, 2005 (“*First Report and Order*”).

<sup>4</sup> *First Report and Order*, at n.74; The FCC interprets “switching” to “include routers, softswitches, and other equipment that may provide addressing and intelligence functions.”

<sup>5</sup> See 47 CFR § 1.7001.

<sup>6</sup> See *First Report and Order*, n.76.

covered regardless of how the interconnected VoIP provider facilitates access to and from the PSTN, whether directly or by making arrangements with a third party.<sup>7</sup>

In addition, the FCC concluded that such providers are “engaged in providing wire or electronic communication switching or transmission services. ... [E]ven VoIP providers that do not own their own underlying transmission facilities nonetheless are engaged in providing ‘switching’ services to their customers.”<sup>8</sup>

#### **B. The “private network” exception**

CALEA contains an important exception for “private networks.” Section 103 specifically excludes “equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.” This exception could be crucial for many providers of utility and municipal networking services, and likely would include many institutional networks within its scope.

### **IV. APPROACHES TO COMPLIANCE AND COSTS**

As outlined in the accompanying matrix, which was prepared by CTC, affected parties have three main technical options for complying with CALEA. These include: (1) an “in-house” option, under which the provider procures, owns, installs, and manages the required mediation and administrative equipment on its own network; (2) a “trusted third party” managed-service option; and (3) a “just-in-time” option, under which the provider contracts with a third-party to deploy the necessary equipment only after it receives an interception request from law enforcement. These options are not necessarily the only ones, nor are they mutually exclusive.

Given the lack of competition among CALEA solution providers, the wide variety of network architectures, and the novelty of the requirements, it is very difficult to make accurate cost estimates. One thing is certain, however – no matter which option a provider selects, it will be expensive. Knowledgeable sources estimate that, for a system serving approximately 15,000 subscribers, the upfront baseline cost for equipment and related services is likely to be in the range of \$70,000 to \$150,000 for an in-house solution, plus potential costs for network upgrade and customization to make the carrier network interoperate with the CALEA equipment. If a provider chooses a “managed service” or a hosted solution involving a “trusted third party,” its upfront costs are likely to exceed \$50,000, and it will also have to pay substantial ongoing management costs, even if law enforcement never requests the provider’s support. The “just-in-time” option, while likely the least expensive approach, will still involve significant upfront costs as the provider must conduct an initial test installation, perhaps involving network upgrade and customization.

---

<sup>7</sup> *First Report and Order*, ¶ 39.

<sup>8</sup> *Id.*, ¶ 42

It is also important to note that considerable time is required to plan, design, and implement CALEA compliance. CALEA compliance solutions must be customized to the carrier's network. There is typically a lead time of weeks or month between the order and delivery of equipment.

Affected providers must generally bear the full cost of CALEA compliance. "Carriers may absorb the costs of CALEA compliance as a necessary cost of doing business, or, where appropriate, recover some portion of their CALEA section 103 implementation costs from their subscribers."<sup>9</sup> CALEA also prohibits covered providers from recovering costs associated with CALEA compliance by imposing intercept charges on law enforcement beyond those necessary to compensate for the cost of the actual interception.

While the costs of compliance with CALEA will be high, the costs of non-compliance could be even higher. Resisting providers are subject to time-consuming and expensive enforcement actions by the FCC and civil actions by the Attorney General / FBI. A non-complying provider may also be subject to fines and civil penalties of up to \$10,000 per day of non-compliance.

#### **V. Section 109(b) Petition Alternative**

As indicated, all covered providers, without exception, must become CALEA-compliant by May 12, 2007. There is, however, a mechanism through which some affected providers may be able to shift the financial burden of their compliance to the DOJ. The DOJ, in turn, must then decide whether to pay these costs or to drop its request for assistance. If it chooses not to pay, the provider will be deemed to be in compliance.

The mechanism for doing so is found within Section 109(b)(1) of CALEA. That provision enables a covered provider to demonstrate to the FCC that it has diligently studied its options and determined that even the least expensive one is not "reasonably achievable." The term "reasonably achievable" is defined in that section in terms of "significant difficulty or expense."

Given the substantial expense of some CALEA compliance options, a section 109(b)(1) petition could present a good cost-saving opportunity for providers that are small or meagerly-capitalized or that face uniquely expensive compliance options. As the FCC has noted:

Commenters to the *Notice* also argue that carriers with smaller subscriber bases are less able to bear the costs of CALEA implementation. To the extent CALEA costs prohibit these carriers from reasonably achieving CALEA compliance, CALEA section 109(b) provides a remedy.<sup>10</sup> . . .

---

<sup>9</sup> Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295, *Second Report and Order and Memorandum Opinion and Order*, FCC 06-56, ¶ 72 (rel. May 12, 2006) ("*Second Report and Order*").

<sup>10</sup> *Second Report and Order*, ¶ 74.

[W]e emphasize that section 109(b)(1)'s due diligence analysis is fact-specific and will take into account, for example, the resources of the petitioner. We recognize that some telecommunications carriers, particularly small telecommunications carriers, may conclude that they cannot afford the efforts required to develop their own solutions. Thus, for example, a small rural telecommunications carrier might provide evidence that the lack of industry standards and solutions, coupled with its lack of financial resources, would justify a finding that the small telecommunications carrier had met its due diligence requirements by proffering only one solution, so long as it is a *bona fide* solution.<sup>11</sup>

Section 109(b) directs the FCC to consider eleven separate factors<sup>12</sup> when determining whether compliance would "impose significant difficulty or expense on the carrier or on the users of the carrier's systems," and section 109(b) petitions should be prepared with those factors in mind. The FCC has stated that it will not consider such petitions until the May 14, 2007, deadline has passed, reasoning that carriers should and will use the intervening time to explore reasonable options for compliance.

Given the extensive due diligence required, it would be prudent for providers that anticipate filing a Section 109(b) petition to take action immediately to explore their options, and should document all such activity in detail for use in the preparation of the petition.

---

<sup>11</sup> *Second Report and Order*, ¶ 51.

<sup>12</sup> Specifically, the FCC is directed to consider:

- (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 [47 USCS § 1002] 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.

47 U.S.C. § 1008(b).

**THE BALLER HERBST LAW GROUP**

A PROFESSIONAL CORPORATION

January 16, 2007

Page 7

**VI. WHAT TO DO NOW**

1. Determine whether your network is subject to CALEA.
2. If so, prepare immediately to file Form 445 (due February 12, 2007) and a system security and integrity plan pursuant to 47 CFR §§ 1.20005-20008 (due March 12, 2007).
3. Discuss your own specific compliance options with technical and legal experts. Even if you anticipate filing a section 109(b) petition, you must demonstrate a high degree of “due diligence” in exploring all available options, and must provide detailed information concerning the costs and burdens associated with the various options.
4. Select a viable option, and commence implementation, OR
5. Begin preparation and documentation of a section 109(b) petition, to be filed with the FCC immediately *after* the May 14, 2007 deadline.

**VII. CONTACTS FOR FURTHER INFORMATION**

**Baller Herbst Law Group** ([www.baller.com](http://www.baller.com))

Jim Baller or Casey Lide

(202) 833-5300

**Columbia Telecommunications Corp.** ([www.internetctc.com](http://www.internetctc.com))

Joanne Hovis or Andrew Afflerbach

(410) 964-5700

**CALEA Compliance Matrix**

	<b>Just-in-Time</b>	<b>Trusted Third Party</b>	<b>In-House Solution</b>
<b>Steps needed to deploy</b>	<ol style="list-style-type: none"> <li>1. survey of existing infrastructure</li> <li>2. determination of number of simultaneous intercepts</li> <li>3. upgrade (if necessary) of existing infrastructure</li> <li>4. design of custom configuration</li> <li>5. test equipment in place and store in nearby third party facility</li> </ol>	<ol style="list-style-type: none"> <li>1. survey of existing infrastructure</li> <li>2. determination of number of simultaneous intercepts</li> <li>3. upgrade (if necessary) of existing infrastructure</li> <li>4. design of custom configuration</li> <li>5. installation of third-party equipment</li> </ol>	<ol style="list-style-type: none"> <li>1. survey of existing infrastructure</li> <li>2. determination of number of intercepts</li> <li>3. design of custom configuration</li> <li>4. upgrade (if necessary) of existing infrastructure</li> <li>5. installation of new equipment</li> </ol>
<b>New equipment typically needed at carrier</b>	<ol style="list-style-type: none"> <li>1. Mediation device belonging to third party (stored in nearby third-party facility)</li> <li>2. Upgrade of network switches (if necessary)</li> <li>3. Upgrade of network software</li> </ol>	<ol style="list-style-type: none"> <li>1. Mediation device (belongs to third party)</li> <li>2. Upgrade of network switches (if necessary)</li> <li>3. Upgrade of network software</li> </ol>	<ol style="list-style-type: none"> <li>1. Mediation device</li> <li>2. Administrative CALEA device</li> <li>3. Upgrade of network switches (if necessary)</li> <li>4. Upgrade of network software</li> </ol>

**THE BALLER HERBST LAW GROUP**

A PROFESSIONAL CORPORATION

January 16, 2007

Page 9

<p><b>Approximate one-time cost of solution</b></p>	<ul style="list-style-type: none"> <li>• \$10,000 for minimum configuration</li> <li>• Depends on number of intercepts</li> <li>• Depends on number of carrier switches</li> <li>• Depends on design of carrier network</li> </ul>	<ul style="list-style-type: none"> <li>• up to \$50,000 to \$100,000 for minimum configuration</li> <li>• Depends on number of intercepts</li> <li>• Depends on number of carrier switches</li> <li>• Depends on design of carrier network</li> </ul>	<ul style="list-style-type: none"> <li>• \$70,000 to \$150,000 baseline price, suitable for 15,000 subscriber system</li> <li>• Depends on number of intercepts</li> <li>• Depends on number of carrier switches</li> <li>• Depends on design of carrier network</li> </ul>
<p><b>Approximate yearly cost of solution</b></p>	<p>~10% of equipment cost (ie. ~\$1000)</p>	<p>~10% of equipment cost (ie. ~\$5,000 to \$10,000)</p>	<p>minimal</p>
<p><b>Upgrade needed for Carrier Infrastructure</b></p>	<ul style="list-style-type: none"> <li>• May require increased capacity within carrier network</li> <li>• Requires modification of network switch software</li> <li>• CALEA equipment provider must be interoperable with carrier switches</li> </ul>	<ul style="list-style-type: none"> <li>• May require increased capacity within carrier network</li> <li>• Requires modification of network switch software</li> <li>• Third party must be interoperable with carrier switches</li> </ul>	<ul style="list-style-type: none"> <li>• May require increased capacity within carrier network</li> <li>• Requires modification of network switch software</li> <li>• CALEA equipment provider must be interoperable with carrier switches</li> </ul>

**THE BALLER HERBST LAW GROUP**

A PROFESSIONAL CORPORATION

January 16, 2007

Page 10

<p><b>Connectivity needed to law enforcement</b></p>	<ul style="list-style-type: none"> <li>• VPN connection from Law Enforcement through Internet</li> <li>• Managed turnkey by third party</li> </ul>	<ul style="list-style-type: none"> <li>• VPN connection from Law Enforcement through Internet</li> <li>• Managed turnkey by third party</li> </ul>	<ul style="list-style-type: none"> <li>• VPN connection from Law Enforcement through Internet</li> </ul>
<p><b>Approximate time to install and activate</b></p>	<ul style="list-style-type: none"> <li>• &gt;3 months</li> <li>• depends on equipment vendor delivery time</li> </ul>	<ul style="list-style-type: none"> <li>• &gt;3 months</li> <li>• depends on equipment vendor delivery time</li> </ul>	<ul style="list-style-type: none"> <li>• &gt;3 months</li> <li>• depends on equipment vendor delivery time</li> </ul>
<p><b>Limitations</b></p>	<ul style="list-style-type: none"> <li>• Risk in “just in time” if not timely</li> <li>• Carrier still liable if third party does not deliver</li> </ul>	<ul style="list-style-type: none"> <li>• May not be as cost-effective for larger carrier</li> <li>• Carrier still liable if third party does not deliver</li> </ul>	<ul style="list-style-type: none"> <li>• High investment for small providers</li> <li>• Carrier must administer compliance</li> </ul>
<p><b>Advantages</b></p>	<ul style="list-style-type: none"> <li>• Turnkey management of compliance and intercepts</li> <li>• Significantly lower cost, especially for smaller carriers</li> </ul>	<ul style="list-style-type: none"> <li>• Turnkey management of compliance and intercepts</li> <li>• Somewhat lower cost, especially for smaller carriers</li> </ul>	<ul style="list-style-type: none"> <li>• Carrier control of all components and response time</li> </ul>