CALEA Compliance

What is CALEA?

The Communications Assistance for Law Enforcement Act ("CALEA") is a statute enacted by Congress in 1994 to require telecommunications carriers to provide law enforcement with certain technical capabilities when they conduct lawful electronic surveillance – also known as a lawful intercept ("LI") — on telecommunications networks. The Federal Communications Commission issued an order in 2005 extending the coverage of CALEA to two-way interconnected VoIP and broadband Internet access. The goal of CALEA is to preserve the ability of law enforcement to conduct LI despite evolutions in network technology. This goal is meant to be achieved while protecting telecommunications subscriber privacy and the ability of telecommunications carriers to launch new services and technologies.

What Entities Does CALEA Apply to?

CALEA applies to "telecommunications carriers," including any entity engaged in the transmission or switching of electronic communications to the public for hire. The term includes providers of wireline and wireless services, as well as providers of facilities-based broadband Internet access and twoway interconnected VoIP.

What does CALEA Require Telecommunications Carriers to Do?

A CALEA telecommunications carrier must essentially ensure that when it is served with a court order for lawful surveillance its network can isolate the communications of the criminal suspect, terrorist or spy identified in the order, and deliver the communications to the law enforcement agency named in the order.

What is a System Security and Integrity Plan?

CALEA requires telecommunications carriers to establish protocols for privacy and security to ensure that lawful intercepts are not compromised. The FCC requires these protocols to be filed with the agency in the form of a "system security and integrity report."

How can a Telecommunications Carrier Comply with CALEA?

A CALEA telecommunications carrier must install a technical solution in its network that delivers to law enforcement the technical capabilities set forth in CALEA Section 103. Section 103 essentially requires the delivery of the suspect's call content and call-identifying information. Industry is permitted to publish technical standards that specify how call content and call-identifying information should be captured and delivered in different types of telecommunications networks. As long as a carrier installs a solution that conforms to one of these "safe harbor" standards the entity will be deemed presumptively compliant with the statute.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau

Are there any Penalties for Failure to Comply?

If a carrier violates a court order for lawful intercept because it lacks the required CALEA capabilities the court may fine the carrier up to $10,000 per day for each day of non-compliance. In addition, the court may order the carrier to bring its network into compliance by a court-specified deadline.

What is a CALEA Trusted Third Party?

A CALEA trusted third party ("TTP") is a company which provides CALEA compliance services to telecommunications carriers on an outsourced basis. The FCC has formally recognized the validity of complying with CALEA through TTPs. Numerous telecommunications carriers of all sizes nationwide have retained TTPs for this purpose. A TTP can provide a carrier with both a CALEA technical solution and a related compliance program. By bundling these two service components and spreading the costs over a nationwide client base the TTP makes CALEA compliance very cost-effective, enabling carriers to concentrate resources on their core businesses.

Are Internet Service Providers Subject to CALEA?

Yes. If the ISP provides paying subscribers with access to the public Internet it is subject to CALEA.

How Can a Carrier Tell if its Switch is CALEA Compliant?

Most if not all traditional and IP switch manufacturers have built lawful intercept software into their switches. However, that software does not by itself make a network CALEA-compliant. The carrier may also need to install a mediation device that can direct the software to capture and re-route the traffic of a named suspect. Beyond that the carrier should test the solution periodically to make sure it still works despite network upgrades and changes in topology.

What is a Lawful Intercept?

A lawful intercept is an investigative technique authorized by a court and implemented by a law enforcement agency to monitor the real-time communications of a criminal suspect, terrorist, or foreign spy. The monitoring may consist of tracking the telephone numbers dialed by the suspect and by those who call the suspect, along with the times, dates, and durations of the calls. Alternatively, a court may issue a "full content order" or wiretap, which authorizes the law enforcement agents to not only collect the suspect's inbound and outbound dialed digits but overhear the person's phone conversations. In the age of IP communications a lawful intercept order may authorize agents to monitor a suspect's broadband Internet sessions. These authorized agents may literally view a computer screen that duplicates the suspect's screen.

Where Does an Intercepted Communication Go?

Typically, a suspect's communications are intercepted at the serving telecommunications switch. From there the communications are routed to a law enforcement monitoring point, which could be located at a nearby state law enforcement agency or a remote federal law enforcement agency.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau

What Happens When a Telecommunications Carrier Receives a Lawful Intercept Order?

First the carrier and/or its trusted third-party CALEA compliance provider must review the order for validity. If the order contains an error (e.g. recites the wrong standard of due process) it should be returned to the law enforcement agency for correction.

Once validated, the order must be implemented. Specifically, the service provider or its trusted third party must arrange for connectivity between the carrier's network and the authorized law enforcement agency, activate the CALEA solution in the carrier's network, ensure the solution delivers the CALEA-required technical capabilities to the law enforcement agency, and deactivate the solution at the court-ordered termination date. Additional tasks are needed to maintain the privacy and security of the intercept and perform certain related FCC-required recordkeeping.

How Does CALEA Protect Subscriber Privacy?

CALEA protects subscriber privacy at every stage of the lawful intercept process.

At the technical standard-setting stage industry lawyers and engineers are permitted to craft intercept standards that limit solutions to delivering only the call content and call-identifying information required by CALEA Section 103. The standards also protect the privacy of non-suspect subscribers.

At the solution development stage equipment vendors may design solutions that conform to an industry standard or achieve the goals of CALEA Section 103 in other privacy-protective ways. At the court order stage CALEA requires telecommunications carriers to confirm the court order is properly authorized before implementing it.

At the implementation stage, pursuant to CALEA, the intercept solution may be activated only when authorized by the carrier's specially-appointed officer or employee. When the solution is activated the carrier controls the type of data transmitted to law enforcement. All the law enforcement agents can do is receive whatever the carrier sends. At the court-ordered intercept termination date the carrier deactivates the solution unless the law enforcement agency has provided a timely renewal order from the court.

Throughout the intercept process CALEA requires the carrier to employ security measures to prevent security breaches and privacy measures to keep the intercept confidential.

What is the Difference Between a Court Order for Lawful Surveillance and a Subpoena?

Law enforcement agencies (LEAs) may require telecommunications carriers to assist criminal investigations in two different ways. Each form of assistance is legally compelled through a separate type of legal instrument, or "due process." The first type of assistance is known as a court order for lawful electronic surveillance. It is also called a "wiretap," "Title III order" or "intercept order." The second type could be a warrant or subpoena such as a "subpoena duces tecum" or "administrative subpoena." These are the basic legal tools that LEAs use to monitor a criminal suspect's use of electronic communications.

The following highlights the differences between an intercept order and a criminal subpoena.

Type of data collected: An intercept order authorizes an LEA to monitor a criminal suspect's communications – such as a phone call or Internet session – in real time. That is, the agent may listen in on the suspect's calls or view the suspect's Internet sessions as they take place. A subpoena is a weaker form of due process. It entitles the agent to collect only "historic" information, such as the suspect's past billing records. Those records reveal who the suspect called and who called the suspect during the targeted billing periods.

Legal standard to collect data: If an LEA wants to conduct an intercept it must apply for the authority from a criminal court. Only if the judge finds that the LEA meets the applicable legal standard will the judge grant the intercept order. For example, if the agent wants to listen to the suspect's voice communications he or she must demonstrate "probable cause" that the suspect is using the voice communications to engage in a felony such as murder or drug dealing. By contrast, if the agent merely wants to see the suspect's past billing records, it can issue a subpoena without the prior approval of a judge. The subpoena must still meet the legal "relevance" standard, meaning the evidence collected is relevant to the criminal investigation. If the LEA fails to meet the applicable due process standard then at the criminal trial stage of the proceeding the suspect may ask the judge to throw out the evidence.

Technical challenge to collect data: Intercepting a suspect's communications requires a technical solution. CALEA sets forth the technical capabilities that telecommunications carriers must build into their networks so they are equipped to comply with intercept orders. Subpoenas may be fulfilled manually or through some automated system used to access the carrier's customer care database and extract the required billing details. If an automated system is used the technical capabilities would not need to comply with any federal or state regulation.

Duration of assistance: An intercept order typically lasts for 30 or 60 days but may be renewed for additional 30 or 60-day periods. A subpoena must be fulfilled within a reasonable time. Once the compliance task is complete the carrier need not worry about a "renewal" of the subpoena per se, but the LEA can always serve a new subpoena on the carrier seeking suspect data reflecting additional billing periods.

Need for privacy: Both intercept orders and criminal subpoenas must be fulfilled on a confidential basis. That means the carrier may not "tip off" the suspect that he or she is being investigated. Otherwise the suspect could flee the jurisdiction, destroy evidence, or even try to kill witnesses.

Other considerations: The above explanation is a simplified description of intercept orders and subpoenas. Many other considerations – legal, technical, and administrative — must be addressed before a carrier is truly prepared to implement these forms of due process.