Neustar® Legal Compliance Services

FAQs for Service Providers

Early in the 1990s, federal and state law enforcement agencies became increasingly concerned that the pace of changes to the telecommunications networks and services was impeding their capability to engage in successful electronic surveillance. In 1994, Congress enacted The Communications Assistance for Law Enforcement Act (CALEA) to address law enforcement's concerns while at the same time address industry concerns that their innovations should not be impeded by law enforcement demands.

In short, CALEA sets technical requirements for deployment of new products and services in the broad communications field. CALEA mandates that a person or entity engaged in switching of wire or electronic communications must ensure that their facilities meet the requirements of CALEA. In 2006, the FCC's rulemaking decided that broadband, VoIP and Internet services had to comply with CALEA.

We've assembled a list of frequently asked questions regarding legal compliance/technical assistance. For more information you can view our recorded webinar, **Legal Compliance: Obligations and Complications for Service Providers** or contact us at **SolutionsTeam@neustar.biz.**

1. **Who must comply with electronic surveillance court orders?**
   Communications services providers are legally obligated by court order to assist law enforcement in carrying out communications surveillance by providing the information, facilities and technical assistance necessary to unobtrusively intercept communications.

   This obligation is independent of any technical obligation imposed by CALEA.

2. **What technical capabilities does CALEA require?**
   CALEA requires service providers to have the ability to:
   - expeditiously isolate the content of all wire and electronic communications to and from a targeted person
   - expeditiously isolate call-identifying information (origin, direction, destination, or termination of each communication generated or received by a targeted person)
   - provide intercepted communications and call-identifying information to law enforcement, preferably by means of an industry-adopted standard
   - carry out intercepts unobtrusively and with a minimum of interference with the target's service
   - ensure that intercepts and pen/traps protect the privacy and security of other people using the service provider

3. **What are the privacy risks of providing legal compliance?**
   Providers must ensure that they only respond to valid lawful process, provide only the information and/or access that is requested and have qualified personnel manage the processes. Subscriber/user privacy and confidentiality are critical to providers' subscriber base as well as the providers' financial success. Providers can easily damage their standing with the courts and/or law enforcement if they do not, or are not able, to assist law enforcement in a timely manner. Providers can also undermine subscriber/public confidence if subscriber privacy is compromised (i.e. more information than is required or the wrong subscriber's information is released).

4. **We have never received a court order for technical assistance. Should we wait until I receive one to do anything?**
   CALEA had compliance dates built into the statute. The first was 1998. With the FCC's decision in 2006–2007, broadband, VoIP and Internet service providers had to come into compliance. It is immaterial whether a provider has never been served with a court order to provide technical assistance. It is impossible to predict when a court order will be served on your company. Given the trends in electronic surveillance, it is likely your company will be served with a court order. If an order is served on your company, you run the risk of fines of up to $10k/day if you're not compliant.

(Continued on reverse side)

5. What are the different types of electronic surveillance methods?

- **Lawful intercept –** electronic surveillance of communications that is authorized by judicial order
- **Trap and trace –** capturing pursuant to court order the phone numbers of incoming calls
- **Pen registers –** capturing pursuant to a court order the phone numbers outgoing calls

Trap and trace and pen registers ("pen/traps") also register the duration of a call as well as whether a call was completed. They do not capture the content of voice or data electronic communications.

6. What is subpoena?

A subpoena is a form of lawful process issued under the authority of a court or administrative agency. A subpoena is used to compel testimony or the production of documents to aid law enforcement agencies in the performance of their duties.

7. What is the FBI's "Going Dark" initiative?

"Going Dark" refers to law enforcement's inability to comprehensively and lawfully collect data and information, conduct electronic surveillance and analyze the raw data due to the rapid evolution of telecommunications and data collection technology and services.

To meet this challenge, key law enforcement and industry representatives have collaborated with the FBI to form a comprehensive, five-pronged National Lawful Intercept Strategy. Key points include:

- modernizing lawful intercept laws
- updating lawful intercept authorities
- increasing law enforcement coordination
- establishing broader industry liaison
- seeking increased funding for these efforts

These proposed additional statutory changes are likely to result in additional burdens on service providers that will make it more difficult and costly to comply with CALEA. See **FBI.gov** and **Electronic Freedom Foundation.**

8. What modifications to the electronic surveillance statutes and Stored Communications Act are being proposed?

They vary according to the proposed legislation. It is clear that these changes may cause providers to adjust to the higher technical requirements by building these technical requirements into their new service offerings.

9. What are the proposed data retention legislations?

The Protecting Children from Internet Pornographers Act of 2011 includes a provision for data retention, requiring service providers to retain basic user profile information (e.g. name, address, IP address and other account information) as well as retain anywhere from months' to years' worth of data and respond forthwith to lawful process for the production of these records.

10. What is a "Trusted Third Party?"

A Trusted Third Party is an agent of a service provider that will carry out on behalf of the service provider the provisioning of technical assistance in response to valid electronic surveillance court orders. Some TTPs, such as Neustar, also produce subscriber information and call detail records, and assist the service provider meet industry adopted CALEA requirements. **Read more.**

Neustar, recognized by the FCC as a Trusted Third Party, can help manage CALEA compliance for your organization and help protect your subscribers' privacy.

For more information, view the webinar, **Legal Compliance: Obligations and Complications for Service Providers.**

Contact us at **SolutionsTeam@neustar.biz.**

About Neustar, Inc.

Neustar, Inc. (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, entertainment, advertising and marketing industries throughout the world. Neustar applies its advanced, secure technologies in routing, addressing and authentication to its customers' data to help them identify new revenue opportunities, network efficiencies, cybersecurity and fraud protection measures. More information is available at **www.neustar.biz.**

Neustar, Inc. Corporate Headquarters
21575 Ridgetop Circle, Sterling, VA 20166 / +1.571.434.5400 / www.neustar.biz /

03/29/2012