COMMUNICATIONS SERVICE PROVIDERS – DO YOU COMPLY WITH INTERNATIONAL LAW ENFORCEMENT ASSISTANCE MANDATES?

March 2017
Communication service providers (CSPs) are generally required to assist law enforcement agency (LEA) investigations. The needed assistance could involve the disclosure of subscriber billing records or the facilitation of real-time lawful electronic surveillance (a lawful “intercept” or “wiretap”). Unfortunately, many CSPs are unsure whether and how to comply with LEA assistance mandates. The confusion tends to multiply as CSPs expand to foreign markets.

It’s no wonder. As communication technologies evolve, it becomes harder to determine which types of networks must produce what types of assistance. Some CSPs are subject to greater assistance obligations than others. Further complicating matters, as service providers extend their networks internationally, they find that different nations have adopted different LEA assistance laws. A common factor applicable to CSPs doing business in all nations: non-compliance with legal mandates is against the law and can lead to serious financial penalties.

A non-compliant service provider may incur liability from two sources. An over-disclosure of communications may provoke subscribers to lodge privacy complaints. An under-disclosure may trigger a government enforcement action.

Smart CSPs adopt law enforcement compliance strategies before launching service and then periodically revisit the plans as their networks grow. The following provides a high-level explanation of how a CSP may approach the issue when operating in the US and expanding to foreign markets.

**CSP Assistance to LEAs in the US**

US CSPs are expected to provide two kinds of LEA assistance: records production and lawful surveillance support.

**Records Production**

Many US law enforcement agencies are authorized to issue subpoenas. These legal tools enable investigators to gather basic evidence such as business records relevant to a crime. Such records are kept by all kinds of companies: banks, airlines, hotels, retailers, etc. When a subpoena is served on a CSP for subscriber billing records, the resulting evidence may point to criminal activity by an individual suspect, or expose an entire crime ring.

The major US wireless carriers receive hundreds of thousands of subpoenas per year. They hire and train special staffs to process the legal instruments. The staffers review each subpoena for validity, and for those found valid, produce the targeted records.

Not all CSPs are able or willing to hire staffs for subpoena processing. Many outsource the function to a specialist firm known as a trusted third party (TTP). A TTP has expertise in law enforcement, privacy protection, and communications networks, can validate and fulfill subpoenas on a CSP’s behalf.

In addition to the mandate of general assistance, certain providers of wire or electronic communications services must comply with the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994 and still the legal mainstay of lawful intercept in the US. CALEA applies to telephone companies, cellular radio carriers, wireline and cable operators of broadband Internet access, and to providers of two-way interconnected VoIP.

The statute exempts various other types of competitors. For example, CALEA does not apply to providers of information services such as email, SMS, web sites, and social media sites. Private networks such as university online research systems that are used only by academics are also exempt.

**Lawful Surveillance: The Fundamentals**

In the US, any “provider of wire or electronic communication service” may receive a court order requiring support for a lawful intercept. The broad term “wire or electronic communication service” covers all types of wireline, wireless and broadband services. When a provider covered by the law receives an intercept order it must provide “all information, facilities, and technical assistance needed to accomplish” the interception. The entity may petition the court for relief if it cannot provide the needed assistance in a “timely” and “reasonable” fashion.
Communications entities subject to CALEA must install lawful surveillance solutions in their networks so they can provision court-ordered intercepts in a standardized manner that makes the surveillance useful to LEAs. The entities must also follow specific protocols to protect the privacy and security of the court-ordered tasks.

An industry member subject to CALEA may comply with the statute using its own resources. Alternatively, it may outsource this function to a Trusted Third Party. A TTP can furnish the CSP with a valid technical solution and operate the solution on the CSP’s behalf to ensure the mandated protocols are met.

Lawful Surveillance Goes “Virtual”
Like so many other aspects of the communications industry, lawful intercept is influenced by “virtualization” – the use of software solutions that perform the same tasks as conventional network hardware. CSPs have increasingly converted their communication services to virtual offerings controlled “in the cloud” from the data centers of tech giants such as Amazon Web Services, IBM, and others. For example, some VoIP providers offer the full range of voice services completely via the cloud. These competitors often wonder how to bring their networks into compliance with CALEA.

While the 1994 Congress that enacted CALEA never contemplated migrations to the cloud, today cloud-based virtual lawful intercept solutions are available. The typical virtual lawful intercept solution consists of software running as a virtual machine in the same data center as the carrier’s VoIP soft switch or session border controller. Once installed, the solution can deliver all the government-required technical capabilities in an efficient, affordable manner. That means CSPs can readily modernize their networks without compromising their LEA compliance programs.

CSP Assistance to LEAs Outside the US
When an American CSP offers its communication services in the European Union or other nations it encounters new mandates for LEA assistance. Each government imposes its own assistance duties. For that reason, trying to serve multiple foreign markets can get complicated. On the other hand, there are commonalities.

Data Retention
Just as US LEAs may serve subpoenas on CSPs to collect the subscriber records of criminal suspects, so may a European Union-based LEA serve a “production order” on a CSP doing business in the jurisdiction to get the same records. An American CSP must be ready to perform the same validation and processing work it carries out in the US.

In most EU member states, service providers are also subject to “data retention” mandates. These regulations require a CSP to save its subscriber records for a minimum number of months or years in case the items are later needed for a criminal investigation. Privacy and security safeguards are required to protect the retained data from unauthorized access.

Notice one key difference between US records production and EU data retention. In the US, if an LEA requests a type of record that the CSP does not store, or a record so old that it is no longer in storage, the CSP may validly reject the request. But in most EU states, as well as any other nation with a data retention mandate, if an LEA requests a record that is supposed to be retained, and the record is no older than the specified retention period, the CSP must comply, or risk an enforcement action.

The more advanced TTPs can handle both US records production and EU data retention while meeting the privacy and security standards. Still, close coordination between the CSP and TTP will be needed to establish protocols that are lawful, reliable, rapid, and efficient.

Lawful Surveillance
In the EU and other nations, CSPs must install solutions to perform real-time surveillance. Each nation’s counterpart to CALEA specifies the technical capabilities to be delivered to LEAs in the given jurisdiction. Unlike the US, the EU does not exempt information services such as social media, SMS or email from surveillance laws.

Surveillance technical standards also vary from one country to the next. A technical standard designed to comply with CALEA cannot be expected to match the surveillance solution blueprints of the EU. Employing the wrong standard is no minor flaw. If a CSP uses a US-based ATIS standard

© 2017 Subsentio, LLC.
to transmit suspect data to an LEA in the EU, where the ETSI\(^2\) standard prevails, the LEA may receive all the packets associated with the suspect’s communications but would be unable to reconstruct the packets to make them intelligible.

International TTPs understand the differences among different surveillance technical standards. They can furnish a CSP with an intercept solution that follows the given country’s legal and technical demands.

Intercept solutions are also keeping pace with virtualization in the EU. Thanks to these efforts, it is now possible for a CSP to deploy a virtual service in the EU and still comply with EU surveillance mandates.

### When Foreign CSPs Enter the US

International service providers that seek to do business in the US are also subject to US law enforcement assistance laws. If a foreign-owned CSP applies for a Federal Communications Commission (FCC) license to serve the US public, the FCC will likely require the competitor to jump through an additional regulatory hoop known as a Team Telecom review.

Team Telecom is an inter-agency task force authorized to ensure that foreign CSPs enter the US market only after demonstrating their commitment to meet the needs of US law enforcement and national security. At a minimum, Team Telecom will expect the CSP to install a valid CALEA solution. Beyond that, the task force may extract other concessions. For example, the applicant may be compelled to name a US citizen or TTP on American soil who is prepared to receive court surveillance orders on the CSP’s behalf. The applicant may even have to equip its network with technical capabilities not expressly mandated by CALEA.

### The Future of CSP Assistance to LEAs

The global spread of crime and terrorism has forced governments worldwide to improve their LEA defenses. Central to that effort is the assistance LEAs receive from CSPs. Because LEAs need two different types of assistance, and because the assistance mandates vary from one country to the next, the CSP’s compliance task can be difficult.

Some CSPs meet their LEA regulatory challenges through in-house resources. Others turn to Trusted Third Parties. Either way, a growing number of compliance options are available. Records production, data retention, and lawful surveillance can all be performed internationally. And the proliferation of virtual networks can be accommodated with virtual surveillance solutions.

As a result, an international CSP today can enjoy the best of both worlds: a technically advanced, far-reaching network and a fully compliant strategy for LEA support.

---

1 The Alliance for Telecommunications Industry Solutions (ATIS) is a membership organization that establishes standards and solutions for the Information and Communications Technology (ICT) industry, based in Washington, DC.

2 The European Telecommunications Standards Institute.