

## Four key areas of focus

Every day, Communication Service Providers (CSP) generate millions of wireless and fixed line phone Call Detail Records (CDRs) and many more Internet records. This is measured in hundreds of millions, and in many cases billions, of events per day. With six to 24 months of retention required, this represents billions of records and terabytes of total data to maintain and manage. In addition, communication providers must quickly execute sophisticated searches across the full repository to retrieve specific records when requested by various government and law enforcement bodies.

The challenges operators face in this area fall into four principals: Collection, Retention, Analyses and Disposal. Here are some best practices to consider in each area:



### COLLECT

**1 All Records must be collected in a timely and secure manner.** To ensure complete investigation for security purposes, it is imperative that all data is collected from the network without any data loss and transferred into the data retention repository ready for immediate query to meet law enforcement demands.

**2 Records should not be modified.** Data under retention may end up being utilized in a court of law. As such, they must not be modified as part of the collection and loading process and a strong “chain of custody” audit trail must be created.

### RETAIN

**3 Data must be held in a secure and tamperproof environment.** Due to the sensitivity of the data stored CSPs, it is essential that once in the repository, access to the data is managed in a secure and diligent manner.

**4 Minimal operational overhead to maintain availability of data.** Data stored for law enforcement purposes typically cannot have any additional business use, i.e. churn analysis. Consequently, being able to store and access this data at a minimal cost is paramount.

**5 Data must be available as needed with minimum delay.** When law enforcement make a request for a report on data under retention, it is important that the result is returned rapidly as there may be either life threatening or items of national importance involved. This negates “off-lining” or archiving retained data.

### ANALYZE

**6 Records must be queried in both pre-defined reports and in an ad-hoc manner.** There are many standard queries used by law enforcement, such as “Who did A call between these dates?” or “What calls were made from cell X at this time?” However, when an investigation has moved on, it is important to be able to make detailed forensic analysis.

**7 Queries should return “Without Undue Delay.”** When queries are submitted by law enforcement, the result must be returned in a predictable and time-critical

manner without introducing a significant cost to the CSP.

**8 Authentication should be used to safeguard data access.** Given the sensitive nature of the data under retention, it is critical that access to the data is not only secured by the system but also has an authentication mechanism to prevent browsing within the data without valid cause.

### DISPOSE

**9 Once retention has expired, records should be deleted in an irretrievable manner.** For data privacy reasons, and for operational costs, it is important that data under retention be made unavailable for query at the point of expiration of the retention period.

**10 Legal Hold should be available on records under investigation.** Whilst maintaining a valid retention, is critical once data is involved in an investigation that data should not be deleted while involved in the case. However, once released from investigation, any data past retention must be made immediately unavailable.

Sensage delivers a scalable, high performance event data management and analysis platform featuring:

- **Diverse collection**—captures and centrally aggregates all event records from all relevant sources including telephony, email messaging, web traffic and custom applications.
- **Efficient management**—Parses and stores event data in a highly compressed format to reduce storage requirements.
- **High-speed, online analysis**—Rapid, pinpoint search through terabytes of data, correlating across event source types.
- **Scalable performance**—exceptional data load and query performance that can be easily expanded.

*Streamline compliance and costs of data retention with Sensage. Visit [www.sensage.com/content/s](http://www.sensage.com/content/s) for a kit of materials on Telco Data Retention.*

COLLECT

RETAIN

ANALYZE

DISPOSE