Mobile Carriers Can Keep Call and Text Metadata for Years



A BleepingComputer item notes that carriers can retain years of call and text metadata, which could reveal relationships, locations and routines if breached. It mentions Cape, a mobile service that deletes call records automatically.

- Carriers can retain call and text metadata for years.
- If breached, this data can expose customers' relationships, locations and daily routines.
- The item examines privacy risks of long-term telecom data retention.
- Cape is presented as a mobile service that reduces exposure by automatically deleting call records.

What the source says

BleepingComputer reports that mobile carriers can keep call and text metadata for years. Even without message content, such records can show who a person communicates with, where they have been and how their day is structured. If a carrier is breached, that history becomes a privacy exposure for its customers.

The item examines the privacy risks of long-term telecom data retention and describes how Cape, a mobile service, limits exposure by automatically deleting call records. The excerpt we reviewed does not give retention periods, breach cases or figures, so we do not cite any.

Why it matters for regulated institutions

For executives, officials and staff with access to sensitive information, communication metadata held by a third party is part of the organisation's risk surface. It sits outside the institution's own controls, yet it can reveal patterns about people and operations.

This is a good moment to ask what telecom data is held about your people, by whom, and for how long.

Practical next step

Treat carrier retention as a third-party and privacy question rather than an incident. Review what your contracts and the carriers' published policies say about retention, and decide whether higher-risk roles need additional measures.

What to do now

1. Review carrier contracts and published policies for how long call and text metadata is retained.
2. Identify roles whose communication patterns are sensitive, such as executives and staff handling critical data.
3. Include telecom providers in third-party risk and privacy assessments.
4. Check whether corporate mobile lines are covered by your data retention and minimisation requirements under PDPL.
5. Brief high-risk staff on what metadata can reveal and on minimising sensitive discussions over standard mobile lines.