What Phone Location Data Can and Cannot Prove

A dot on a map looks precise, but the weight of mobile location evidence depends on its source, timestamp, accuracy estimate and how it was collected. This note explains how to identify the record behind each point and what it takes to connect a device's location to its owner. Our mobile examiners have had their evidence accepted in court.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/insights/mobile-location-evidence-limits/

A phone may contain several records associated with place, and each describes its own kind of event. Some are device sensor estimates. Others are cached searches, application defaults, cell sector associations, photo metadata, paired device records, or account activity. Accuracy values often describe an estimated uncertainty radius, which the examiner distinguishes from a tested error for that individual observation. The examiner should identify how each record was created before placing it on a map.

Identify the Record, Time Basis and Measurement Conditions

Potential sources include device location databases, application records, WiFi observations, cell site or sector records, navigation history, photographs, health activity, vehicle systems, cloud account data, carrier records, and third party business systems. Each has different retention, precision, clock behavior, collection limits, and meaning. A cell sector association describes a coverage area, distinct from a GPS fix. A geotag may describe the media or an edit rather than the device at capture. An account event may reflect remote access. A complete finding pairs each coordinate with its source context.

Normalize Time Before Drawing a Route

Mobile databases may store UTC, local time, offset values, Apple or Unix epochs, server time, device time, or application specific formats. Daylight saving transitions and travel can create apparent reversals. The analysis retains the original value and conversion rule, then compares it with known events and independent records.

The examiner preserves original coordinates, timestamps and accuracy fields, identifies whether each record reflects device, account, network or content location, tests for sync, cache, import, edit and platform processing effects, compares independent sources before placing a person at a location, and states the precision and the gaps on the map and in the report.

Connecting a Device to a Person

A device or account can be shared, left behind, remotely accessed, or carried by someone else. Location evidence may establish that a device generated or stored a record. Attribution to a particular person normally requires corroborating facts supplied by the record or established elsewhere.

Primary Sources and Technical References

- NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics https://csrc.nist.gov/pubs/sp/800/101/r1/final
- Apple, Location Services and Privacy https://support.apple.com/en-us/102515

© 2026 Global Digital Forensics, Inc. All rights reserved.

Get a Free Consultation

The first call is a free consultation with a senior examiner. We review the matter, the evidence and the deadline, and outline the collection and analysis it needs. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.