

Geolocation Evidence

Geolocation evidence comes from diverse sources like GPS, Wi-Fi, cell, EXIF, and app data. This guide addresses their different reliability, how to correlate them onto a timeline, and the importance of honest confidence in presenting findings. It covers common mistakes, technical limitations, and when to involve a digital forensic expert.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31. <https://e-discovery.uk/library/geolocation-evidence>

GEOLOCATIONEVIDENCE · A GUIDE FOR UK LAWYERS Geolocation Evidence GPS, Wi-Fi, Cell, EXIF and App Data: Converging Sources, Honest Confidence COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES MULTI-SOURCE GEOLOCATION LOCATION ACCURACY & CONFIDENCE CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: many sources, different reliability 03 The location sources and how they work 04 Accuracy and the confidence ladder 05 Collecting and correlating location onto a timeline 06 Convergence, contradiction and honest limits 07 Deployment: presence, alibi, movement and privacy 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary The headline point: location comes from many sources of very different accuracy, GPS, Wi-Fi, cell, photo metadata, app and cloud histories, and the reliable answer comes not from one source but from making several converge on a timeline, each stated at its honest confidence rather than asserted with false precision.

§ 02 · FIRST PRINCIPLES The problem in plain English: many sources, different reliability

§ 03 · THE SOURCES The location sources and how they work GPS WI-FI CELL EXIF APP / CLOUD

§ 04 · THECONFIDENCELADDER Accuracy and the confidence ladder

§ 05 · COLLECTINGANDCORRELATING Collecting and correlating location onto a timeline

§ 06 · CONVERGENCEANDHONESTLIMITS Convergence, contradiction and honest limits

§ 07 · DEPLOYMENT Deployment: presence, alibi, movement and privacy

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives LOCATION CLOUD NETWORK VEHICLE / COUNTERPART / DELETED / SOURCE PLATFORMS O PER AT OR WEARABLE CCTV RECOVERABLE DEVICE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THECELLRECORDTHATWASNOTAPINPOINT EXAMPLE2 ·

THE CONTRADICTION THAT REVEALED THE TRUTH EXAMPLE 3 ·
THE PROPORTIONATE SLICE OF AN INTRUSIVE HISTORY

§ 10 · WHERE IT GOES WRONG Common mistakes and technical limitations Common mistakes
Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask
your client Ask your opponent (or a data holder) Ask your e Discovery / forensic provider
SUGGESTED WORDING · INSTRUCTION FOR GEOLOCATION ANALYSIS

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The
geolocation checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Which location source is the most
reliable? The other side says a cell record puts our client at a specific address. Is that right?
Does location data prove our client was there, or just their phone? The sources disagree. Does
that ruin the evidence? Can we just get our opponent's full location history? There is no location
data for the key period. Does that mean our client was not there?

§ 14 · REFERENCE Glossary EXIF Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab
Speak to a forensic examiner, not a salesperson. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

Which location source is the most reliable?

It depends on the conditions, but as a rule a good GPS fix is the most precise (metres), Wi-Fi positioning is moderate (tens of metres), and cell-tower data is only approximate (an area), with photograph EXIF as good as the fix the camera had (§3, §4). No single source is authoritative in all conditions, which is why the method is not to pick the best source but to converge several, each at its honest confidence (§6).

The other side says a cell record puts our client at a specific address. Is that right?

Almost certainly overstated: a cell-tower connection places a phone within that cell's coverage, an area that can span hundreds of metres or kilometres, not at a specific point (§4, Example 1). It is one of the commonest over claims. A specific address is merely one place within the cell's area, and more accurate sources, GPS, Wi-Fi, EXIF, should be brought in to test whether the client was actually there.

Does location data prove our client was there, or just their phone?

Strictly, the device (§6): phones are lent, left and shared, so location records place the device, and attribution to the person requires corroboration. Usually the device is with its owner, but not always (Example 2), so the honest finding distinguishes the two and reaches the person through other evidence, other location sources, messages, CCTV, a wearable, converging on the same conclusion.

The sources disagree. Does that ruin the evidence?

Not at all, it can be the most revealing part: contradiction between sources is examined, not ignored (§6, Example 2). A conflict may show a device was left behind, a fix was stale, or clocks differed, and resolving it often exposes the truth. What is not acceptable is silently dropping the inconvenient source. Honest handling of contradiction is a strength of a proper geolocation analysis, not a weakness.

Can we just get our opponent's full location history?

You should not, and usually cannot proportionately: a person's assembled movement history is among the most intrusive evidence there is, engaging serious UK GDPR duties (§7). Collection is scoped tightly to the relevant place and window and minimised, and the wider history is neither gathered nor exposed (Example 3). The narrow, proportionate slice is both the lawful course and, being focused and unassailable, the more persuasive one.

There is no location data for the key period. Does that mean our client was not there?

No: absence of a location record is not proof of absence from a place (§4, §6). Location services may have been off, the device may have been elsewhere or without signal, or the record may simply not have been kept. Gaps are explained, not over-read. And the estate may still answer the question, a vehicle, a wearable, CCTV or a counterpart's record may place the person where the device's own data is silent (§8). cflab. uk · e-discovery. uk ©2026
Computer Forensics Lab Ltd · cflab.uk · e-discovery.uk · info@cflab.uk · +44 (0)20 7164 6915
Page 15 of 17

Source: <https://e-discovery.uk/library/geolocation-evidence>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.