



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Geolocation Evidence

GPS, Wi-Fi, Cell, EXIF and App Data: Converging Sources, Honest Confidence

Where was a person at a given moment? It is one of the most frequently decisive questions in litigation, and modern devices answer it many times over, from different sources of very different reliability. A phone knows its position from GPS satellites, from the Wi-Fi networks around it, and from the cell towers it connects to; photographs carry the coordinates where they were taken embedded in their metadata; countless apps record location in the background; cars, wearables and cloud services all keep their own location histories. Each of these is a witness to place, but each speaks with a different accuracy, from a GPS fix good to a few metres down to a cell connection that only narrows position to an area, and none is infallible. The skill in geolocation evidence is not finding a single location source but making several converge: assembling the independent records onto one timeline, letting them corroborate each other, and stating the confidence of each honestly rather than asserting a false precision. This guide sets out for UK lawyers the location sources, how they are collected and correlated, how their accuracy differs, and how a converged location picture is built and honestly bounded.

🕒 Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Geolocation work draws together the location sources across a matter: device GPS, Wi-Fi and cell records, photograph metadata, app and cloud location histories, and vehicle and wearable data, correlated onto a single timeline with the accuracy and confidence of each source stated honestly, and reported under CPR Part 35 and CrimPR Part 19 in a way that survives scrutiny precisely because it does not overstate.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

MULTI-SOURCE GEOLOCATION

LOCATION ACCURACY & CONFIDENCE

CPR PART 35 EXPERT REPORTS

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

§ 0 1 · 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.

The sources (§3): GPS fixes good to metres, Wi-Fi positioning to tens of metres, cell connections only to an area, photograph EXIF coordinates, and app and cloud location histories, each a distinct witness to place. **Confidence (§4):** the sources sit on a ladder of accuracy from precise to approximate, and a location is only as strong as the source it rests on, so each is labelled with its real accuracy. **Collecting and correlating (§5):** the location records are collected from device, apps, cloud and providers and assembled onto one timeline, so they can be compared and corroborated. **Convergence (§6):** the reliable finding is where independent sources agree; where they contradict, the conflict is examined and explained, not resolved by picking the convenient one. **Deployment (§7):** proving presence or absence, testing an alibi, showing movement, and the significant UK GDPR and privacy dimension of assembling a person's location history.

- **Many witnesses to place:** GPS, Wi-Fi, cell, photo EXIF, app and cloud data each record location differently.
- **Accuracy varies widely:** from a few metres (GPS) to a whole area (cell), so every location carries a confidence.
- **Convergence is the method:** the reliable answer is where independent sources agree on a timeline.
- **State confidence honestly:** label each source's real accuracy; never assert a precision the source cannot bear.
- **Location is sensitive:** assembling a movement history engages significant UK GDPR and privacy duties.

Independent location sources converging on one timeline

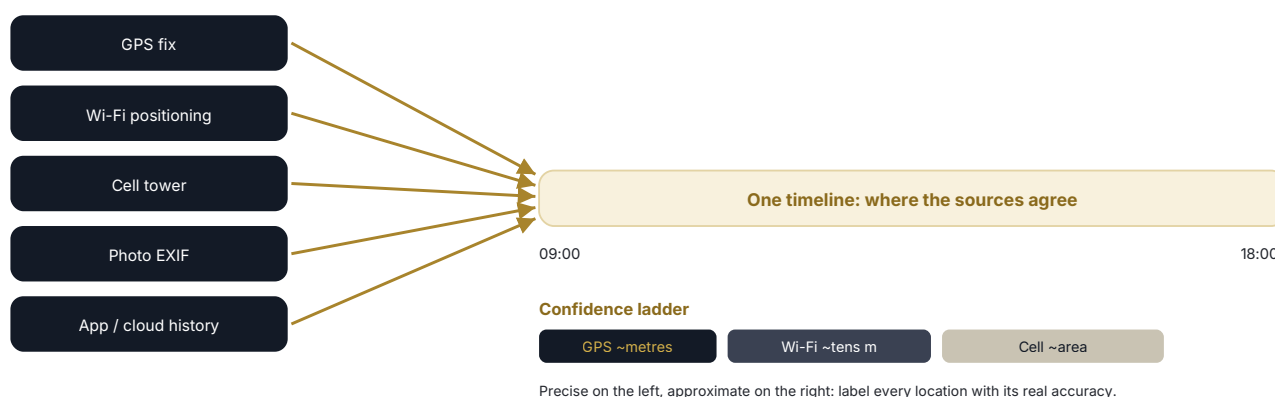


Figure 1 - the method is convergence: independent sources of differing accuracy assembled onto one timeline, each carrying its honest confidence, with agreement carrying the weight.

The problem in plain English: many sources, different reliability

The question "where was this person?" feels like it should have a single answer, and modern technology seems to promise one: a dot on a map. But the promise is misleading, because that dot can come from any of several sources, and they are not equally reliable. A GPS fix, when the device had a clear view of the sky, can be accurate to a few metres. A position estimated from surrounding Wi-Fi networks is good to perhaps tens of metres in a well-mapped area, and much worse elsewhere. A location derived from which cell tower a phone connected to may only place it somewhere within an area of hundreds of metres or several kilometres, depending on the density of towers. A photograph's embedded coordinates are as good as the GPS fix the camera had at the time. And an app's recorded location may be any of these, or a coarse approximation, depending on how the app asked for it. To treat all of these as the same, a location, is the fundamental error.

The discipline of geolocation evidence, therefore, is not to hunt for one authoritative source but to gather the several that exist and make them converge. Each source is a witness of a certain reliability; assembled together onto one timeline, they corroborate or contradict each other, and where independent sources of good accuracy agree, the finding is strong. Where they conflict, the conflict itself is informative and must be examined, not smoothed over by choosing the convenient source. And every location must be stated at its true confidence: a GPS fix as precise, a cell connection as approximate, never a cell record dressed up as a pinpoint. Add to this that a person's assembled location history is among the most privacy-intrusive evidence there is, engaging serious UK GDPR duties, and the shape of the task is clear: gather widely, correlate carefully, state confidence honestly, and handle with proportion. This guide sets out how.

§ 0 3 · THE SOURCES

The location sources and how they work

- **GPS and satellite positioning:** the device computes its position from satellites, accurate to a few metres with a clear sky, degraded indoors and among tall buildings: the most precise source when available, recorded by the device and by apps that request precise location.
- **Wi-Fi positioning:** the device estimates position from the known locations of surrounding Wi-Fi networks, good to tens of metres in well-mapped areas, weaker elsewhere: a common source indoors and in cities where GPS struggles.
- **Cell-tower data:** the network records which cell a phone connected to, placing it within that cell's coverage, an area from a few hundred metres in cities to several kilometres in the countryside: approximate, held by the network operator, and obtained by lawful process (an area, not a point).
- **Photograph metadata (EXIF):** photographs taken on location-enabled devices embed the coordinates of capture in their EXIF metadata, as accurate as the device's fix at the time: a location tied to a specific image and moment (guide 108's metadata discipline).
- **App and cloud location histories:** mapping, social, transport and countless other apps, and platform-level location histories, record positions over time, of varying accuracy, held on the device and in the cloud: a rich, continuous source reached through the device and the account (guides 111 to 114).

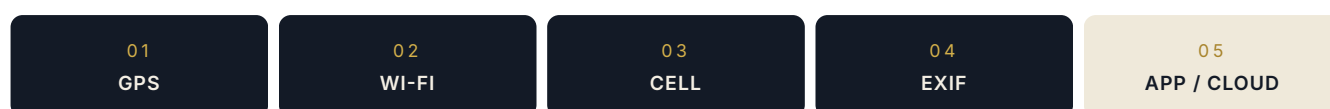


Figure 2 - the five principal location sources, each with its own accuracy and its own holder, gathered together rather than relied on singly.

Accuracy and the confidence ladder

- **Accuracy is a spectrum:** location sources range from precise (a good GPS fix, metres) through moderate (Wi-Fi, tens of metres) to approximate (a cell connection, an area): the location's evidential weight set by where its source sits on this ladder.
- **Every location carries a confidence:** a coordinate without an accuracy figure is incomplete, many sources record their own estimated accuracy, and that confidence is stated with the location, so precise and approximate sources are not treated alike.
- **A cell is an area, not a point:** the commonest overclaim, plotting a cell-tower record as a pinpoint when it means only "somewhere in this cell's coverage": cell data presented as the area it truly is (§3).
- **Conditions degrade accuracy:** indoors, among tall buildings, in poor coverage, even GPS degrades and Wi-Fi and cell become coarse: the conditions considered, so a fix is not assumed precise regardless of circumstance.
- **Confidence compounds on convergence:** where several independent sources of differing accuracy agree, the combined confidence exceeds any one alone: the strength of convergence, and the reason the method gathers many sources (§6).

Collecting and correlating location onto a timeline

- **Gather from every source:** the device's own location records, the apps' histories, the photographs' EXIF, the cloud platforms' location data and, by lawful process, the network's cell data, collected from across the estate, not from one place (§8).
- **Collect lawfully and proportionately:** device and app data by consent or authority, cloud data through the account or provider, cell data by lawful process, each obtained by the right route and scoped to the relevant period and question, because location is highly intrusive (§7, guide 20).
- **Normalise onto one timeline:** the disparate records, with their different formats and time bases, reconciled to a common timeline and clock (guides 96, 108), so locations from different sources can be compared at the same moments.
- **Label each with its source and confidence:** every plotted location tagged with where it came from and its accuracy, so the timeline shows not just points but their reliability (§4): the honesty built into the record.
- **Preserve provenance:** the integrity and origin of each location record preserved and documented (guides 2, 3), so the converged picture rests on sound, attributable data and can be explained and reproduced.

Convergence, contradiction and honest limits

- **Agreement is strength:** where independent sources, a GPS fix, an EXIF coordinate, an app history, agree on a location at a time, the finding is robust because the sources corroborate each other: the converged conclusion the method exists to produce.
- **Contradiction is informative:** where sources disagree, the conflict is examined, a device left at home while its owner travelled, a photograph with a stale fix, clock error between sources, not resolved by silently preferring the convenient one (guide 100's honest-limits discipline).
- **The device is not the person:** location records place the device, and attribution to the person requires corroboration, since phones are lent, left and shared: the same account-to-person limit as elsewhere (guide 105), applied to place.
- **Absence and gaps:** no location record for a period is not proof of absence from a place, location services may be off, the device elsewhere: gaps explained, not read as evidence of location (§4).
- **State confidence, not certainty:** the converged finding expressed at its true confidence, "the sources place the device here, to this accuracy, at this time", rather than as a false pinpoint, because overstated location evidence collapses under scrutiny (§4).

Deployment: presence, alibi, movement and privacy

- **Proving presence or absence:** the converged location placing a device, and by corroboration a person, at or away from a place at a time, in matters from criminal presence to civil breach to family disputes, stated at honest confidence (guide 96).
- **Testing an alibi:** the location sources tested against an account of whereabouts, corroborating a truthful alibi or exposing a false one, with contradictions between sources examined rather than ignored (§6).
- **Showing movement and pattern:** the location history revealing routes, visits and patterns over time, in fraud, stalking, employment and other matters, deployed proportionately given its intrusiveness (guide 98).
- **Corroborating other evidence:** location aligned with messages, transactions, CCTV (guide 121), vehicle (guide 122) and wearable (guide 123) data, so place, time and activity reinforce one another on a single timeline.
- **Privacy and UK GDPR:** assembling a person's location history is among the most intrusive things litigation does, engaging significant UK GDPR duties, lawful basis, necessity, proportionality and minimisation, so the collection is scoped tightly to the relevant question and period and the wider movement record is not gathered or exposed needlessly (§5, guide 20).

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: location is the most distributed evidence of all, held in more places than almost any other, which is precisely why convergence works. The device holds GPS, Wi-Fi and app location records and photograph EXIF; the cloud platforms hold location histories, photo libraries with coordinates and app data server-side; the network operator holds cell-connection data; and around these, the vehicle holds journeys (guide 122), the wearable holds routes (guide 123), other devices and counterparties hold their own location records and the messages that mention place, and CCTV holds the person in view (guide 121). The discipline is to gather from as many of these as the question proportionately warrants, because each is a witness of different accuracy and independence, and their convergence, or their contradiction, is the evidence. When the device's own record is missing, the cloud history holds it; when GPS is absent, cell and Wi-Fi place it approximately; when the phone was left behind, the vehicle, the wearable or the CCTV corroborates the person; and no single silent source defeats a location question that several others can still answer.

LOCATION SOURCE	DEVICE	CLOUD PLATFORMS	NETWORK OPERATOR	VEHICLE / WEARABLE	COUNTERPART / CCTV	DELETED / RECOVERABLE
GPS fixes	Y: precise	Y: synced history	n/a	Y: journeys/ routes	n/a	Varies
Wi-Fi position	Y	Sometimes	n/a	Sometimes	n/a	Varies
Cell connection	Device logs (limited)	n/a	Y: area, by process	n/a	n/a	Operator retention
Photo EXIF	Y: in image	Y: cloud photos	n/a	n/a	Shared copies	Recoverable if deleted
App / platform history	Y: app data	Y: account history	n/a	App-linked	Shared location	Varies

Fallback strategy in one line: gather location from every proportionate source and converge them; when one is missing, silent or coarse, the cloud, the network, the vehicle, the wearable or CCTV supplies or corroborates the place.

Worked examples

EXAMPLE 1 · THE CELL RECORD THAT WAS NOT A PINPOINT

An opponent's expert plotted a single cell-tower connection as a precise dot on a map and asserted that it placed the defendant at a specific address. The §4 confidence discipline dismantled the overclaim: the cell record meant only that the phone had connected to a tower whose coverage was an area of several hundred metres in that urban location, an area, not a point, and the asserted address was merely one of many places within it. The §6 convergence then did the real work: the device's own GPS and app-location records for the same window, collected from the phone, placed it, to a few metres, at a different location entirely, and a geotagged photograph (§3 EXIF) corroborated the GPS. Three independent, more accurate sources converged against a single over-plotted cell record. The honest presentation, cell as an area, GPS and EXIF as precise and agreed, was decisive. The lesson is §4's: a cell connection is an area, not a pinpoint, and converged precise sources honestly stated defeat a single approximate source dressed up as certainty.

EXAMPLE 2 · THE CONTRADICTION THAT REVEALED THE TRUTH

A claimant's phone location appeared to support his account of being at a site, but something did not fit. The §6 discipline of examining contradiction rather than smoothing it resolved the case: while the phone's records placed it at the site, the §8 estate told a fuller story, his vehicle's telematics (guide 122) showed the car parked at his home throughout, his wearable (guide 123) recorded a continuous sleep period at home across the same window, and geotagged photographs from his own account placed him elsewhere. The phone had been left at the site by a colleague; the person was at home. The apparent phone location, taken alone, would have been misleading, but the convergence of vehicle, wearable and photograph evidence against it exposed that the device was not with its owner, precisely the §6 device-is-not-the-person limit. The lesson is §6's: contradiction between sources is not noise to be ignored but evidence to be examined, and it is convergence across independent sources, not any single record, that reveals the truth.

EXAMPLE 3 · THE PROPORTIONATE SLICE OF AN INTRUSIVE HISTORY

A matter required proof of where a person had been during three specific hours on one day. The temptation was to obtain their entire location history, months of continuous movement, but the §7 proportionality and UK GDPR discipline confined the collection to the relevant window: the device's GPS and app-location records, the cloud platform's location history and a geotagged photograph, all scoped to those three hours, were collected and converged, and the vast remainder of the person's intrusive movement history was neither gathered nor exposed. The converged sources answered the question, to honest confidence, for the relevant hours alone. The narrow, proportionate collection was both lawful and, in fact, more persuasive, focused and unassailable rather than a sprawling intrusion inviting challenge. The lesson is §7's: a person's location history is among the most private evidence there is, and the disciplined, proportionate slice, scoped to the question and minimised, is both the lawful course and the stronger one.

Common mistakes and technical limitations

Common mistakes

- **Plotting a cell record as a pinpoint:** the classic overclaim, an area presented as a precise point (Example 1, §4).
- **Relying on a single source:** one location record trusted alone where convergence would confirm or contradict it (Example 2, §6).
- **Ignoring confidence:** coordinates plotted without their accuracy, so precise and approximate sources look alike (§4).
- **Smoothing over contradiction:** a conflicting source silently dropped rather than examined (Example 2, §6).
- **Assuming the device is the person:** device location attributed to its owner without corroboration (Example 2, §6).
- **Reading gaps as absence:** no location record treated as proof the person was not there (§6).
- **Trusting a stale EXIF fix:** a photograph's coordinates assumed precise when the device's fix was poor (§3).
- **Over-collecting:** a person's whole movement history gathered where a scoped window was proportionate (Example 3, §7).

Technical limitations

- **Accuracy varies by source and condition:** from metres to kilometres, and degraded indoors and in poor coverage: every location carries a real, and sometimes coarse, confidence (§4).
- **Cell data is approximate:** it places a phone in an area, never at a point: an inherent limit, not a defect to be argued away (§3).
- **Attribution needs corroboration:** location places the device; the person requires other evidence (§6).
- **Sources can conflict:** devices are left and shared, fixes go stale, clocks differ: contradiction is expected and examined (§6).
- **Cell and cloud need process and time:** operator and provider data is obtained by lawful process on legal timelines, and operator retention is finite (§5, §8).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What is the precise location question, which place, which times, so collection is scoped tightly to it rather than sweeping a whole movement history?
- What devices, apps, accounts, vehicles and wearables might hold location for that window, so every proportionate source is considered?
- Is there a photograph, message or other record that independently fixes place and time?

Ask your opponent (or a data holder)

- Please preserve and disclose all location records for [device/person] for [specific window], including device GPS, Wi-Fi and app-location data, platform location history and geotagged photographs, each with its recorded accuracy.
- Please confirm the sources and accuracy of any location asserted, and in particular whether any location plotted as a point is in fact cell-tower data representing an area.
- Please preserve any vehicle, wearable and cloud location data for the same window.

Ask your eDiscovery / forensic provider

- What is each location source here, and what is its real accuracy, on the confidence ladder?
- Do the independent sources converge or contradict, and how is any conflict explained?
- How do we scope this to the relevant window and minimise an intrusive movement history?

SUGGESTED WORDING · INSTRUCTION FOR A GEOLOCATION ANALYSIS

"We instruct you to establish, to honest confidence, the location of the device or person at Schedule 1 for the specific period stated, and no wider. Please: (1) identify and collect, lawfully and proportionately, every relevant location source for that window, device GPS, Wi-Fi and app-location records, photograph EXIF, platform and cloud location history, and, where justified, cell-tower data by lawful process, and any vehicle and wearable location, scoping the collection to the relevant period and minimising the wider movement history; (2) normalise the records onto a single timeline and common clock, and label each location with its source and its real accuracy; (3) determine where the independent sources converge and where they contradict, examining and explaining any conflict rather than preferring a convenient source; (4) state the finding at its true confidence, presenting cell data as the area it represents and never as a pinpoint, and distinguishing the location of the device from the presence of the person, which requires corroboration; and (5) treat the assembled location data as highly sensitive personal data throughout, handled with necessity, proportionality and minimisation."

Checklist and red flags · When to involve a digital forensic expert

The geolocation checklist

- ☐ The location question scoped to specific place(s) and time(s)
- ☐ Every proportionate source identified across the estate
- ☐ Collection lawful, proportionate and minimised to the window
- ☐ Records normalised onto one timeline and common clock
- ☐ Each location labelled with its source and real accuracy
- ☐ Cell data presented as an area, never a pinpoint
- ☐ Convergence and contradiction both examined and explained
- ☐ Device location distinguished from presence of the person
- ☐ Gaps explained, not read as absence
- ☐ Assembled location history handled as highly sensitive data

Red flags

- A cell record plotted as a precise point: Example 1.
- A single location source relied on with no corroboration: Example 2.
- Coordinates presented with no accuracy or confidence.
- A contradicting source quietly dropped.
- Device location asserted as the person's presence.
- A data gap read as proof of absence.
- A whole movement history collected for a narrow question.

When to involve a digital forensic expert

Whenever location is genuinely in issue, because the discipline is specialist: the expert identifies every proportionate source across the estate, collects each lawfully, and, crucially, assigns each its true accuracy on the confidence ladder rather than treating all locations alike (§4, §5); at correlation, where the sources are normalised onto one timeline and their convergence or contradiction is examined and honestly explained (Examples 1 and 2, §6); at the guard against overclaim, where cell data is kept to the area it represents, device location is distinguished from the person, and gaps are not read as absence (§6); at proportionality, where the collection is scoped and the intrusive wider history minimised (Example 3, §7); and at deployment, where the converged, honestly-bounded finding is explained under CPR Part 35 or CrimPR Part 19 and survives scrutiny precisely because it claims only what the sources support. Through **cflab.uk** and **e-discovery.uk**, geolocation work converges many witnesses of different reliability into one honest picture: because the reliable answer to "where were they?" comes not from a single dot but from independent sources agreeing, each stated at its true confidence.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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 overclaims. 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).

§ 1 4 · REFERENCE

Glossary

GPS

Satellite positioning, precise to metres with a clear sky.

Wi-Fi positioning

Location estimated from nearby known networks, tens of metres.

Cell-tower data

The tower a phone used, placing it in an area, not a point.

EXIF

Photograph metadata, including capture coordinates.

Location history

An app or platform record of positions over time.

Confidence ladder

The ranking of sources by accuracy, precise to approximate.

Convergence

Independent sources agreeing on a location at a time.

Accuracy figure

The estimated error attached to a location reading.

Attribution

Linking a device's location to a specific person.

Timeline correlation

Placing multiple sources on one common time base.

Sources and authoritative references

The geolocation disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (multi-source geolocation, cell-site and device location analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (location collection and timeline correlation as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (including cell-site analysis and its limits): gov.uk, [FSR Code](https://gov.uk/fsr-code) · ISO/IEC 27037: iso.org, 27037
- ICO, location data and UK GDPR guidance (necessity, proportionality and minimisation): ico.org.uk · NIST SP 800-101 Rev. 1, Mobile Device Forensics: csrc.nist.gov, SP 800-101
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35

DISCLAIMER

This publication provides general information about geolocation evidence as at August 2026. The accuracy of location sources varies by technology, condition and circumstance, and location data places a device, not certainly a person; findings depend on convergence, corroboration and honest confidence. Assembling location history is highly intrusive and must be handled lawfully and proportionately. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Geolocation work at the laboratory is built on convergence and honest confidence. The location question is scoped tightly to the relevant place and window, and every proportionate source across the estate is identified and collected lawfully, device GPS, Wi-Fi and app data, photograph EXIF, cloud and platform location history, and, where justified, cell-tower data by lawful process, alongside vehicle and wearable location where they bear on the question (guides 122, 123). The records are normalised onto one timeline and a common clock, and, crucially, each location is labelled with its source and its real accuracy on the confidence ladder, so a precise GPS fix and an approximate cell connection are never treated alike, and cell data is presented as the area it truly represents rather than a pinpoint (Example 1). Where the independent sources converge, the finding is robust; where they contradict, the conflict is examined and explained, and the device is distinguished from the person (Example 2). The intrusive wider movement history is minimised throughout, because a person's location is among the most sensitive data litigation touches (Example 3). Reports run under CPR Part 35 or CrimPR Part 19 and survive scrutiny because they claim only what the sources support. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is constant: the reliable answer to where someone was comes from independent sources agreeing, each stated at its true confidence.



INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@cflab.uk

E-DISCOVERY

e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace