COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# Vehicle Infotainment and Telematics Forensics

## The Car as a Witness: Connected Phones, Journeys, Doors and Events

A modern car is a computer that happens to have wheels, and it remembers a great deal. The infotainment system records every phone that was paired to it, and often copies across the contacts, call logs and text messages of those phones; the navigation system logs destinations, routes and recent journeys; the vehicle's own modules record door openings, ignition cycles, gear selections, speeds, seatbelt and light status, and the sharp events that precede a collision. Telematics and connected-car services add a cloud dimension, journeys, locations and vehicle status reported back to the manufacturer or an insurer. For a lawyer, the car is a witness that can place a person and a device at a time and place, corroborate or refute an account of a journey, and reconstruct the seconds around a collision, if the data is preserved and extracted correctly, and if its limits are understood. This guide sets out for UK lawyers what vehicle systems record, how the data is preserved and extracted, and how it is deployed and honestly bounded.

⏱ Estimated reading time: 24 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. Vehicle forensics is a growing part of its work: infotainment and navigation extraction, recovery of paired-device data and journey history, event and module data where accessible, and the correlation of vehicle records with phones and telematics: reported under CPR Part 35 and CrimPR Part 19, with the extraction method and the honest limits of what a given vehicle yields set out plainly.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | INFOTAINMENT & TELEMATICS | PAIRED-DEVICE & JOURNEY RECOVERY | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

The headline point: a modern car records paired phones, journeys, door and ignition events and often collision data, and reports much of it to the cloud, so the vehicle can place a person and a device at a time and place, if the data is preserved and extracted correctly and its limits are honestly stated.

**What it records (§3):** the infotainment system stores paired devices and frequently copies their contacts, call logs and messages; navigation logs destinations and journeys; and vehicle modules record doors, ignition, gear, speed and the sharp events around a collision. **Telematics (§4):** connected-car and insurer telematics report journeys, locations and vehicle status to the cloud, a second source with its own retention, reachable through the account or provider. **Preserving and extracting (§5):** vehicle data is extracted through the infotainment system and diagnostic ports with specialist tools, and, because much of it can be altered or lost by continued use, the vehicle and any connected accounts are preserved promptly. **Correlation and limits (§6):** vehicle data is strongest when corroborated with the paired phone and the telematics cloud, and its limits, what a given make records, and the fact that presence of a car is not presence of a person, are stated honestly. **Deployment (§7):** journeys and collision reconstruction, placing a device and a person, and the UK GDPR and privacy questions that vehicle data, including passengers' paired phones, raises.

- **The car is a witness:** it records paired phones, journeys, door and ignition events and often collision data.
- **Phones leave a copy behind:** infotainment often copies contacts, call logs and messages from paired devices.
- **Telematics adds a cloud layer:** connected-car and insurer services report journeys and status server-side.
- **Correlate, do not assume:** vehicle data is strongest cross-checked with the phone and cloud; a car is not a person.
- **Preserve promptly:** continued use overwrites journey and paired-device data, so the vehicle and accounts are secured early.

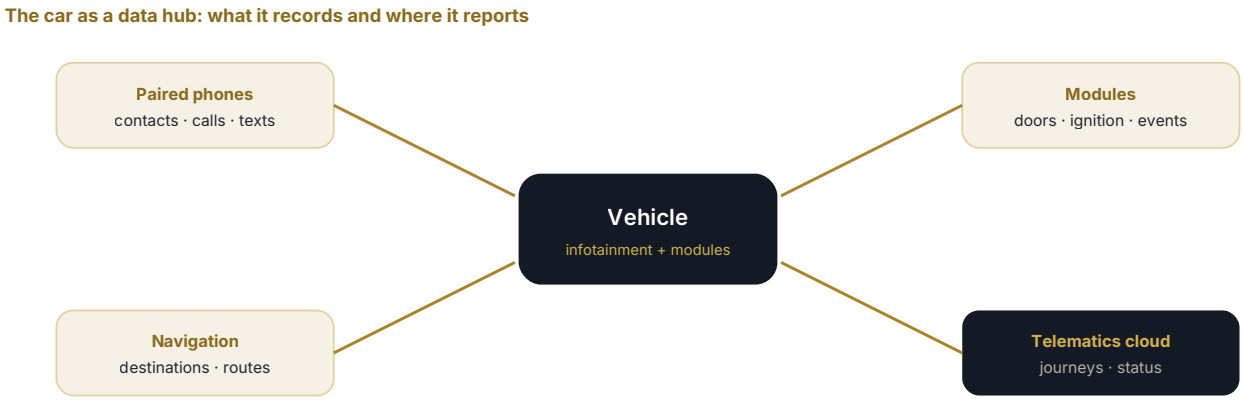


*Figure 1 - the vehicle sits at the centre of a small evidence estate: the phones paired to it, the journeys it logged, the events its modules recorded, and the telematics it reported to the cloud.*

§ 0 2 · FIRST PRINCIPLES

# The problem in plain English: the car remembers

People think of a car as a means of transport, not as a computer keeping records, and they are surprised by how much it retains. Plug a phone into a modern car, even once, and the infotainment system remembers the phone, and often copies over its address book, its recent calls and sometimes its text messages, so that they are available on the car's screen. Enter a destination into the navigation and the car keeps it, along with the route and a history of recent journeys. And beneath the touchscreen, the vehicle's control modules are quietly logging the mechanical facts of every trip: when the doors opened, when the ignition turned, which gear was selected, how fast it was going, and, in the crucial moments before a collision, a detailed record of speed, braking and impact.

For a lawyer this makes the car a witness of unusual richness. It can show that a particular phone, and therefore probably a particular person, was in the vehicle at a given time; it can confirm or contradict an account of where someone drove; it can reconstruct the seconds around a crash with data no eyewitness could supply. But it is a witness that must be handled with care and with honesty. Different makes and models record very different things, so what one car yields another will not. Continued driving overwrites journey and paired-device history, so preservation matters. And, most importantly, the car records the car: that a vehicle went somewhere, or that a phone was paired, does not by itself prove who was driving or who was present. This guide sets out what the car remembers, how to get it out intact, and how to use it without overclaiming.

§ 0 3 · WHAT VEHICLE SYSTEMS RECORD

# What vehicle systems record: infotainment, navigation and modules

- **Paired-device records:** the infotainment system stores a list of every device paired to it, with identifiers and often timestamps of pairing and connection, and frequently copies across the phone's contacts, call logs and, on some systems, text messages: a record of which phones were in the car and when, and a copy of their data left behind on the vehicle.
- **Navigation history:** entered destinations, recent and favourite locations, calculated routes and journey logs, with times: a record of where the vehicle was taken and when, and of the places its user searched for (guide 124's location discipline).
- **Vehicle module data:** the control modules record door openings, ignition cycles, gear selection, speed, seatbelt and light status and similar operational events, with timing: the mechanical narrative of each trip, held in the vehicle's own electronics.
- **Event and collision data:** many vehicles record the seconds around a sharp event or collision, speeds, braking, steering, impact, in an event data recorder: the detailed reconstruction data a collision case turns on, where the vehicle is so equipped.
- **Wide variation by make and model:** what a given vehicle records, and whether it is extractable, varies enormously between manufacturers, models and years: the honest first step is to establish what this particular vehicle holds, not to assume a uniform standard (§6).

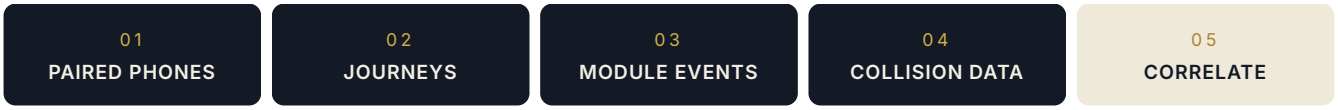


*Figure 2 - the vehicle's four record types, brought together and corroborated against the phone and telematics rather than relied on alone.*

§ 0 4 · TELEMATICS AND CONNECTED-CAR DATA

# Telematics and connected-car cloud data

- **Manufacturer connected services:** modern vehicles report to the manufacturer's cloud through built-in connectivity, journeys, locations, vehicle status, remote-lock and start events and diagnostics, accessible through the owner's connected-car account or the manufacturer by lawful request: a cloud record independent of the car itself.
- **Insurance telematics:** insurer black-box and app-based telematics record journeys, locations, speeds and driving behaviour to price and monitor policies, held by the insurer: a detailed movement and behaviour record obtainable from the insurer by request or order.
- **Companion apps:** the manufacturer's smartphone app that mirrors vehicle status, location and journey history to the owner's phone and account: a further copy of the connected-car data, on the phone and in the account.
- **Retention and access:** telematics retention and the access route (account, app, provider disclosure) vary by manufacturer and insurer and are established per source, with the cloud copy sometimes outlasting the vehicle's own overwritten history (§8): the second source secured before its own retention expires.
- **The account is the reach:** as with other cloud sources (guides 111 to 114), the connected-car and telematics data is reached through the controlling account by consent or through the provider by lawful process, quite independent of physical access to the vehicle.

§ 0 5 · PRESERVING AND EXTRACTING

# Preserving and extracting vehicle data

- **Preserve promptly:** continued use of the vehicle overwrites journey history, adds and removes paired devices and can cycle event buffers, so the vehicle is secured and its connected accounts preserved as early as the matter allows (guide 95's preservation urgency, for cars).
- **Specialist extraction:** vehicle data is extracted through the infotainment unit and the diagnostic port using specialist vehicle-forensic tools that support the specific make and model, or by removing and reading the relevant module, an area of genuine specialism, not a generic phone extraction.
- **Integrity and documentation:** the extraction conducted to preserve integrity, the data hashed and the method and tool documented, so the vehicle evidence is as sound and explainable as any other (guides 2, 3).
- **The cloud in parallel:** the telematics and connected-car account preserved and collected alongside the vehicle (§4), because it is independent, may hold more, and may outlast the car's own overwritten records.
- **Coverage varies and is stated:** tool support for a given vehicle varies, and some data is not extractable at all: the honest scope of what can and cannot be obtained from this vehicle established at the outset, so expectations are realistic (guide 100's honest-limits discipline).

§ 0 6 · CORRELATION AND HONEST LIMITS

# Correlation, corroboration and honest limits

- **The car is not the person:** the central honest limit, that vehicle data shows what the vehicle did and which device was paired, not who was driving or present: attribution to a person requires corroboration, and the finding is stated at the level the evidence supports (guide 105's account-to-person discipline, for vehicles).
- **Corroborate with the phone:** the paired phone's own records, its call logs, location and messages, cross-checked against the car's copy and pairing times, so the two sources confirm each other and the device is placed in the car (guide 96's timeline discipline).
- **Corroborate with telematics:** the connected-car and insurer cloud data cross-checked against the vehicle's own journey and event records, so the movement account is confirmed from two independent sources (§4).
- **Timing and clocks:** vehicle and module clocks, like DVR clocks (guide 121 §6), can be wrong and are checked and reconciled with external references before the data is placed on the timeline.
- **Make-and-model reality:** the finding bounded by what this specific vehicle records and what the tools can extract, so the report says what was obtained and what was not, rather than implying a completeness the vehicle does not offer (§3).

§ 0 7 · DEPLOYMENT

# Deployment: journeys, collisions, presence and privacy

- **Journeys and presence:** the vehicle's navigation and telematics placing the car at times and places, and the paired-device records placing a phone, and probably a person, in it, corroborating or refuting an account of movement, in disputes from alibis to fraud to family matters (guide 124).
- **Collision reconstruction:** event and module data reconstructing the seconds around a crash, speed, braking, impact, seatbelt and light status, as objective evidence in personal-injury, insurance and criminal driving cases, deployed with the specialist reconstruction it supports.
- **The insurance-fraud context:** telematics and vehicle data exposing staged or exaggerated collisions, journeys inconsistent with a claim, or a vehicle not where it was said to be, the objective record against the account (guide 98).
- **Attribution stated honestly:** presence of the car and pairing of a device presented as what they are, evidence of the vehicle and device, corroborated to reach the person, and never overstated as direct proof of who was driving (§6).
- **UK GDPR and passengers:** vehicle data includes the personal data of the owner and of passengers whose phones were paired, so its collection, disclosure and use engage the UK GDPR, and the private data of third parties, passengers' copied contacts and messages, is handled with data-protection care and minimisation (guide 20).

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the vehicle is one node, and almost everything it records is reflected in the phone that was paired to it and the cloud it reported to. The car holds the paired-device copies, the navigation history and the module and event data. But the paired phone holds the original of the contacts, calls and messages the car copied, plus its own location record; the telematics and connected-car cloud hold the journeys and status independently, often with longer retention than the car's own overwriting history; the manufacturer's companion app on the phone mirrors the same; the insurer holds the black-box data; and the counterparties, the people called, the passengers, hold their side. The discipline is to preserve the vehicle, the phone and the cloud account together, because each corroborates the others and each has its own retention and its own gaps, and the attribution to a person that the car alone cannot give comes from the phone and the cloud beside it. When the car's journey history has overwritten, the telematics cloud may still hold it; when the vehicle cannot be extracted, the paired phone holds the copied data; and when both are silent, the insurer's black box may answer.

| EVIDENCE | THE VEHICLE | PAIRED PHONE | TELEMATICS / CONNECTED CLOUD | INSURER BLACK BOX | COMPANION APP | DELETED / OVERWRITTEN |
|---|---|---|---|---|---|---|
| **Which phone, when** | Y: pairing records | Y: its own logs | Driver-profile links | Sometimes | Account devices | Varies |
| **Contacts / calls / messages** | Y: copied to car | Y: the original | n/a | n/a | n/a | Deleted-message recovery |
| **Journeys / locations** | Y: nav history | Phone location | Y: cloud journeys | Y: trip data | Y: app history | Overwritten in car; cloud may hold |
| **Doors / ignition / events** | Y: modules | n/a | Some status | Behaviour data | Status snapshots | Event buffers cycle |
| **Collision seconds** | Y: event recorder | Crash detection | Some report | Y: impact data | n/a | Buffer-limited |

Fallback strategy in one line: preserve the vehicle, the paired phone and the telematics cloud together; each corroborates the others, the cloud often outlasts the car's overwritten history, and the phone supplies the attribution the car alone cannot.

§ 0 9 · IN THE WILD

# Worked examples

### EXAMPLE 1 · THE PAIRED PHONE THAT PLACED A PERSON IN THE CAR

A defendant in a criminal matter denied having been in a particular vehicle on the night in question. The vehicle's infotainment system told a different story: the §3 paired-device records showed his phone, identified by its unique identifier, paired to the car and connected during the relevant window, and the system had copied across his recent call log, which matched calls his own phone records confirmed for that period. The §6 corroboration was careful and honest: the car proved the phone was in it, and the phone records proved the phone was his and active then, and together, not alone, they placed him in the vehicle. The report was explicit that the car recorded the device, not the person, and that the attribution rested on the phone corroboration. The combined evidence was compelling precisely because it did not overclaim. The lesson is §6's: the car places the device, the phone places the person, and the two together are stronger and more honest than either overstated alone.

### EXAMPLE 2 · THE OVERWRITTEN JOURNEY AND THE TELEMATICS THAT KEPT IT

A commercial dispute turned on whether a company vehicle had made a particular delivery run. By the time the vehicle was examined, weeks later, its navigation history had overwritten, the journey in question long since cycled out by ordinary use, a §5 preservation-delay problem. But the §4 telematics carried the case: the vehicle was fitted with an insurer black box, and the insurer, on request, disclosed the trip data for the relevant date, which held the journey, its route and its timings intact, independent of the car's own overwritten record. The §8 estate had preserved what the vehicle had lost. The lesson is §8's: the car's own history overwrites with use, but the telematics cloud is a separate source with its own retention, and preserving the cloud account, or reaching the insurer, recovers what the vehicle itself no longer holds.

### EXAMPLE 3 · THE COLLISION SECONDS AND THE HONEST RECONSTRUCTION

A personal-injury claim disputed how a collision had happened, each driver blaming the other. One vehicle was equipped with an event data recorder, and the §3 module and event data were extracted with specialist tools: the seconds before impact showed the vehicle's speed, a late and heavy braking input, and the impact itself, an objective record no eyewitness could match. The §5 extraction was documented and hashed, and the §6 clock was checked and reconciled with the other vehicle's data and the scene. The reconstruction was presented within honest limits: the recorder captured this vehicle's dynamics, not the other's intentions, and the finding was confined to what the data showed. The objective seconds resolved the mechanics of the collision that the drivers' accounts could not. The lesson is that vehicle event data is powerful and objective, and most persuasive when extracted properly and confined honestly to what it actually records.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **Assuming the car equals the driver:** the central error, treating pairing or presence of the vehicle as proof of who was driving or present, without the phone corroboration (Example 1, §6).
- **Delay letting journeys overwrite:** the vehicle used for weeks before examination, its navigation and paired-device history cycled out (Example 2, §5).
- **Ignoring the telematics cloud:** only the car examined, the connected-car or insurer data, often richer and longer-retained, never sought (§4, §8).
- **Assuming a uniform standard:** a make-and-model's records assumed from another vehicle, when what cars record varies enormously (§3).
- **Generic extraction attempts:** phone-forensic tools or ad-hoc methods used where specialist vehicle-forensic capability for the specific model is needed (§5).
- **Trusting the vehicle clock:** module and infotainment timestamps relied on without a clock check (§6).
- **Overclaiming collision data:** one vehicle's event data used to assert the other driver's actions it never recorded (Example 3).
- **Passengers' data mishandled:** copied contacts and messages of passengers swept up and disclosed without data-protection care (§7).

## Technical limitations

- **Recording varies enormously:** what a vehicle holds and whether it is extractable depends on make, model and year: no uniform standard, and the scope is stated per vehicle (§3).
- **Tool support is patchy:** vehicle-forensic tools support some vehicles and not others; some data is not extractable at all: the honest limit, stated (§5).
- **Use overwrites:** journey and paired-device history cycles with continued use; event buffers are finite: preservation is time-sensitive (§5).
- **Attribution needs corroboration:** the car cannot, alone, say who was driving; the phone and other sources supply the person (§6).
- **Cloud access needs process:** telematics and connected-car data is reached through the account or the provider on legal timelines, not instantly (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- What is the make, model and year of the vehicle, and is it still in use, so we know what it may record and whether history is overwriting?
- Is the vehicle fitted with connected-car services or an insurer black box, and who holds those accounts?
- Which phones were paired to it, and are those phones available to corroborate the vehicle data?

## Ask your opponent (or a data holder)

- Please preserve the vehicle and its data without further use that may overwrite journey or paired-device history, and confirm the make, model and year and any connected-car or telematics services fitted.
- Please preserve and disclose the vehicle's infotainment, navigation, module and event data for [period], and the connected-car or insurer telematics data for the same period, including journeys, locations, paired devices and vehicle status.
- Please identify all phones paired to the vehicle and preserve any that are within your control.

## Ask your eDiscovery / forensic provider

- What does this specific make and model record, and what can the tools actually extract?
- What does the telematics or connected-car cloud hold, and does it outlast the car's own history?
- How is the vehicle data corroborated with the paired phone, and what does it honestly prove about the person?

### SUGGESTED WORDING · INSTRUCTION FOR A VEHICLE-DATA EXAMINATION

> "We instruct you to preserve and examine the electronic data of the vehicle identified at Schedule 1. Please: (1) advise what data this make, model and year is capable of recording and what can be extracted with available tools, and preserve the vehicle promptly against overwriting of journey and paired-device history; (2) extract, preserving integrity and documenting the method, the infotainment paired-device records (including any copied contacts, call logs and messages), navigation and journey history, module data (doors, ignition, gear, speed and similar) and any event or collision data; (3) preserve and collect in parallel the connected-car and insurer telematics data through the relevant account or provider, noting its retention; (4) correlate the vehicle data with the paired phone(s) and the telematics cloud, and state honestly the level at which the evidence supports attribution to a person, distinguishing presence of the vehicle and pairing of a device from identification of the driver; and (5) handle any third-party personal data (including passengers' copied contacts and messages) with data minimisation. Report what was and was not obtainable from this vehicle."

§ 12 · QUICK CONTROL

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

## The vehicle-data checklist

- ☐ Make, model and year identified; recording capability established
- ☐ Vehicle preserved promptly against overwriting with use
- ☐ Connected-car and insurer telematics accounts identified and preserved
- ☐ Paired phones identified and preserved for corroboration
- ☐ Extraction by specialist tools supporting the specific vehicle
- ☐ Infotainment, navigation, module and event data extracted and hashed
- ☐ Vehicle and module clocks checked and reconciled
- ☐ Vehicle data corroborated with phone and telematics
- ☐ Attribution stated honestly: car and device, not assumed driver
- ☐ Third-party (passenger) personal data minimised and protected

## Red flags

- Presence of the car or a paired device asserted as proof of the driver: Example 1's avoided overclaim.
- A vehicle driven for weeks before examination, history overwritten: Example 2.
- Only the car examined, the telematics cloud ignored.
- A make-and-model's records assumed from a different vehicle.
- Generic or ad-hoc extraction of a vehicle needing specialist tools.
- Vehicle timestamps relied on with no clock check.
- Passengers' copied contacts and messages disclosed without care.

## When to involve a digital forensic expert

Early, to establish what this specific vehicle records and to preserve it before continued use overwrites the journey and paired-device history, and to secure the telematics account before its retention expires (Example 2, §5); at extraction, where specialist vehicle-forensic tools for the make and model pull the infotainment, navigation, module and event data intact and documented (Example 3); at correlation, where the vehicle data is cross-checked with the paired phone and the telematics cloud and the attribution to a person is stated honestly rather than assumed (Example 1, §6); and at deployment, where journeys, collision reconstruction and presence are explained under CPR Part 35 or CrimPR Part 19, with the car-is-not-the-driver limit made explicit and passengers' data protected. Through **cflab.uk** and **e-discovery.uk**, vehicle forensics pairs the car with the phone and the cloud and confines the finding to what the data honestly shows: because the car is a rich witness, but it testifies to the vehicle, and the person comes from the sources beside it.

§ 13 · COMMON QUESTIONS

# Frequently asked questions

### What can a car actually tell us?

Often a great deal: which phones were paired to it and when, and frequently copies of those phones' contacts, calls and messages; the destinations and journeys entered into its navigation; door, ignition, gear and speed events from its modules; and, on many vehicles, the seconds around a collision (§3). But it varies enormously by make and model, so the honest first step is to establish what this particular vehicle records and what can be extracted (§5).

### Does the car prove who was driving?

No, and this is the key limit: the car records the vehicle and the paired device, not the person (§6, Example 1). It can show a phone was in the car and where the car went, but attribution to a driver or passenger requires corroboration, usually the paired phone's own records placing it with a person. The honest finding is stated at the level the evidence supports: the car places the device, the phone places the person.

### The car has been driven since. Is the data gone?

Some of it may be: continued use overwrites journey history, changes the paired-device list and cycles event buffers (§5). But the telematics or connected-car cloud is a separate source with its own retention and often holds the journeys the car itself has overwritten (§4, Example 2), and the paired phone holds the originals of the copied data. Preserve promptly, but a used car is not always a lost case.

### Can we get the journey data from anywhere other than the car?

Yes: the manufacturer's connected-car cloud and the insurer's telematics black box both record journeys, locations and status independently of the vehicle, reachable through the owner's account or the provider by lawful request (§4, §8). The companion app on the phone mirrors much of it too. These cloud sources often outlast the car's own overwriting history, which is why they are preserved in parallel.

### Is the collision data reliable?

Where a vehicle has an event data recorder, its record of the seconds around a crash, speed, braking, impact, is objective and powerful (§3, Example 3), extracted with specialist tools and documented. Its limits are honest: it records that vehicle's dynamics, not the other driver's intentions, and its clock is checked and reconciled. Presented within those limits, it resolves the mechanics of a collision that eyewitness accounts cannot.

### What about the privacy of passengers whose phones were paired?

It must be respected: a car often copies the contacts, call logs and messages of every phone paired to it, including passengers', so vehicle data can contain third parties' personal data (§7). Its collection, disclosure and use engage the UK GDPR, and that third-party data is handled with minimisation and protected, disclosing the relevant material and shielding the rest, much as with any device holding others' private information.

§ 14 · REFERENCE

# Glossary

**Infotainment**
The car's screen system, storing paired devices and their data.

**Paired device**
A phone connected to the car, recorded with identifiers and times.

**Navigation history**
Destinations, routes and journeys logged by the car.

**Control module**
Vehicle electronics logging doors, ignition, speed and events.

**Event data recorder**
A module recording the seconds around a collision.

**Telematics**
Journey and behaviour data reported to a cloud service.

**Connected car**
A vehicle reporting status and location to the manufacturer.

**Black box**
An insurer telematics device recording journeys and driving.

**Diagnostic port**
The vehicle port through which data is extracted.

**Companion app**
The manufacturer's app mirroring vehicle data to a phone.

## Sources and authoritative references

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

- cflab.uk, digital forensics services (infotainment and telematics extraction, paired-device and journey recovery, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (vehicle and telematics preservation and collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (vehicle and digital evidence): gov.uk, FSR Code · ISO/IEC 27037 (identification, collection and preservation): iso.org, 27037
- NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics (extraction principles applied to vehicle systems): csrc.nist.gov, SP 800-101 · ICO, UK GDPR guidance (connected and telematics data): ico.org.uk
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Vehicle work at the laboratory begins by establishing what this particular make, model and year records and what the tools can actually extract, and by preserving promptly, both the vehicle, before continued use overwrites its journey and paired-device history, and the connected-car or insurer telematics account, before its own retention expires (Example 2). Extraction uses specialist vehicle-forensic capability for the specific vehicle to pull the infotainment paired-device records and copied phone data, the navigation and journey history, the module data and any event or collision recorder, preserving integrity and documenting the method (Example 3). The vehicle data is then corroborated with the paired phone and the telematics cloud, and the finding is confined honestly to what it supports: the car places the vehicle and the device, and the phone beside it places the person, an attribution stated at its true level and never overstated (Example 1). Third-party personal data, the passengers whose phones were paired, is handled with minimisation. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a car is central to a matter, the first steps are to preserve it and its telematics account and to find out, honestly, what this particular vehicle remembers.

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