COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iOS Spyware, Stalkerware and Mobile Compromise

When the Phone Itself Is the Weapon: Detecting Covert Surveillance, and the Duty of Care It Demands

Sometimes the phone is not the source of evidence but the instrument of harm. Covert surveillance of a mobile takes several forms: consumer stalkerware installed by someone with physical access, most often an abusive partner tracking a victim; the misuse of legitimate features such as shared location, Find My, or an account the other person controls; and, rarely, sophisticated spyware. Detecting compromise is genuinely difficult on a locked-down platform like iOS, and this work carries an unusual duty of care, because the person in front of you may be at real risk. Handling a suspected-stalkerware phone wrongly can alert the perpetrator and escalate danger, so victim safety comes before evidence-gathering. This guide sets out for UK lawyers how iOS devices are covertly surveilled, how compromise is detected and its limits, and, above all, how to approach a suspected-compromise case safely, so that the investigation protects the person before it examines the phone.

⏱ 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. Suspected-compromise work is a sensitive strand of its mobile practice: detecting stalkerware, the misuse of legitimate tracking features, and other covert surveillance on iOS, understanding the real limits of detection, and, above all, handling these cases with a duty of care that puts the safety of a potential victim before evidence-gathering. The analysis is careful, safety-led and honest about its limits, and is reported under CPR Part 35 and CrimPR Part 19, in coordination with the safeguarding the situation requires.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | STALKERWARE & COMPROMISE DETECTION | SAFETY-LED, VICTIM-CENTRED APPROACH | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: sometimes the phone is not the source of evidence but the instrument of harm, covertly surveilled through consumer stalkerware, the misuse of legitimate features like shared location and Find My, or rare sophisticated spyware, and this work carries an unusual duty of care, because victim safety comes before evidence-gathering.

How devices are surveilled (§3): stalkerware installed with physical access (often by an abusive partner), the misuse of shared location, Find My and controlled accounts, and, rarely, sophisticated spyware. **Detection and limits (§4):** detecting compromise is genuinely hard on a locked-down platform, so detection has real limits, and absence of evidence is not proof of safety. **Safety first (§5):** the paramount duty, because handling a suspected-stalkerware phone wrongly can alert the perpetrator and escalate danger, so the victim's safety leads. **Interpretation (§6):** findings, and the limits of detection, stated honestly, without false reassurance or false alarm. **Deployment (§7):** protecting the person first, then gathering evidence, in coordination with safeguarding.

- **The phone as the weapon:** covert surveillance, not a source, is the issue.
- **Three forms:** stalkerware, misused legitimate features, and rare spyware.
- **Detection is hard:** a locked-down platform limits what can be found.
- **Safety before evidence:** wrong handling can escalate danger; the victim comes first.
- **Honest limits:** absence of findings is not proof the phone is clean.

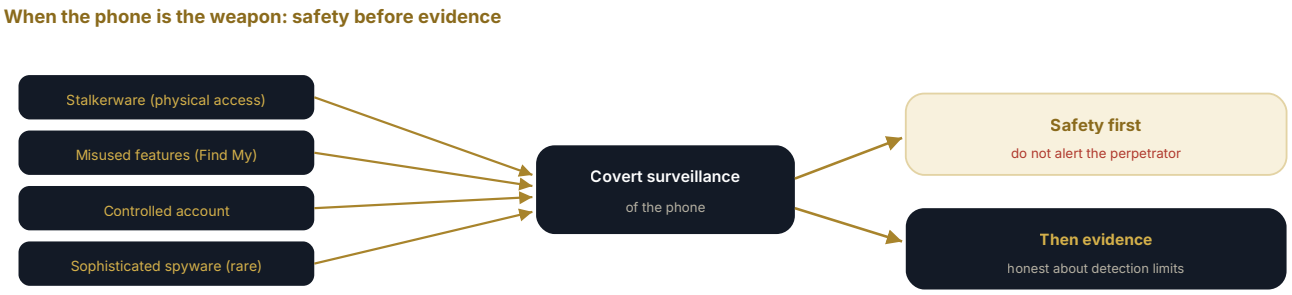

Figure 1 - covert surveillance takes several forms, and a suspected-compromise case is led by the person's safety, do not alert the perpetrator, before evidence-gathering, which is honest about the limits of detection.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: when the phone is the weapon

Every other guide in this block treats the phone as a source of evidence about what its owner did. This one is different, because sometimes the phone is not evidence of the owner's conduct but the instrument of someone else's harm against them. A person may come to a lawyer believing, often rightly, that their phone is being used to watch them: to track their location, read their messages, listen to their calls, or monitor their movements, by someone who means them harm. This is a common and serious feature of domestic abuse and stalking, and it changes the nature of the work entirely, because now the phone is the weapon and the client is the target.

Covert surveillance of an iPhone takes a few main forms, and it is important to be realistic about their relative likelihood. By far the most common is consumer stalkerware, monitoring software installed by someone who had physical access to the device, typically an abusive partner or ex-partner who knows or can guess the passcode. Almost as common, and often overlooked, is not malware at all but the misuse of entirely legitimate features: shared location, Find My, family-sharing arrangements, or simply an Apple account that the abuser set up or controls, all of which can be used to monitor a person without any "hacking" at all. Rarest, and usually the preserve of state-level actors, is sophisticated spyware. Two hard truths shape the work. The first is that detection is genuinely difficult: iOS is a locked-down platform that limits what monitoring software can do but also limits what an examiner can inspect, so a clean scan is reassuring but never conclusive, and absence of evidence is not evidence of absence. The second, and paramount, is that this work carries an unusual and serious duty of care. The person in front of you may be at real physical risk, and handling their phone wrongly, running a scan the perpetrator is alerted to, removing monitoring in a way that provokes them, or even asking the wrong question at the wrong time, can escalate the danger. So in these cases, victim safety comes before evidence-gathering, always. This guide sets out how iOS devices are covertly surveilled, how compromise is detected and its limits, and, above all, how to approach a suspected-compromise case safely.

§ 0 3 · HOW DEVICES ARE SURVEILLED

How iOS devices are covertly surveilled

- **Consumer stalkerware:** monitoring apps installed by someone with physical access and the passcode, most often an abusive partner, tracking location, messages and activity, the most common form (guide 139): the installed monitor.
- **Misused legitimate features:** shared location, Find My, and family-sharing used to monitor a person without any malware, an under-recognised and very common route (guide 152): the feature abused.
- **Controlled account:** an Apple account the abuser set up or controls giving access to the victim's synced data and device (guide 158), so the account itself is the surveillance: the account as the tap.
- **Sophisticated spyware:** advanced spyware, rare and usually state-level, capable of deep compromise, considered where the threat profile genuinely warrants it (guide 139): the rare, serious threat.
- **Physical and network vectors:** physical tracking devices and network-level interception as adjacent threats, so the whole surveillance picture, not just the phone's software, is considered (guide 130): the wider vectors.

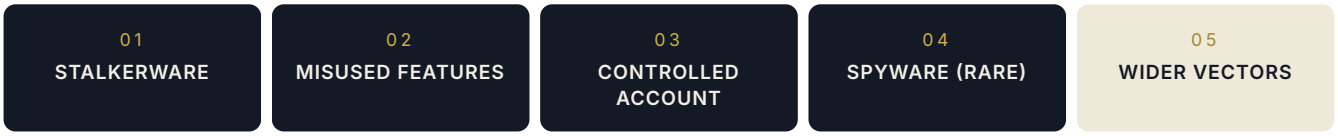

Figure 2 - covert surveillance of an iPhone: most often stalkerware or misused legitimate features and controlled accounts, rarely sophisticated spyware, with physical and network vectors alongside.

§ 0 4 · DETECTING COMPROMISE

Detecting compromise, and its limits

- **Check the legitimate features first:** the shared-location, Find My, family-sharing and account settings checked first, since the most common surveillance is not malware at all (§3): the settings review.
- **Examine for stalkerware:** the device examined for monitoring software and its traces, within what iOS allows an examiner to inspect (guide 139): the malware examination.
- **Review the account and devices:** the account's associated devices, sign-ins and sharing reviewed (guide 158), so covert access through the account is found: the account review.
- **Consider indicators, not just signatures:** behavioural and contextual indicators of compromise considered alongside known signatures, since novel or sophisticated tools evade signatures (guide 100): the indicator-based view.
- **Detection is genuinely limited:** iOS's locked-down nature limiting inspection, so a clean result is reassuring but not conclusive, and this limit is stated honestly (§6): the honest detection limit.

§ 0 5 · SAFETY FIRST

Safety first: the duty of care

- **Victim safety before evidence:** the paramount principle, that the safety of a person at risk comes before gathering evidence, so every step is weighed for its effect on their safety first (guide 20's care theme): the overriding duty.
- **Do not alert the perpetrator:** the risk that examining or cleaning the phone alerts the abuser and escalates danger, so actions are chosen not to tip them off (§3): the no-alert principle.
- **Preserve before removing:** evidence of surveillance preserved before anything is removed, and removal timed and planned with safety in mind, not done reflexively (guide 2): the preserve-then-plan approach.
- **Coordinate with safeguarding:** the work coordinated with the safeguarding, support and, where appropriate, police response, so the technical steps fit a safety plan (guide 100): the coordinated response.
- **Consider a safe device:** where risk is high, using a separate, safe device for communications, so the victim is not communicating on a monitored phone (§7): the safe channel.

§ 0 6 · INTERPRETATION AND HONEST LIMITS

Interpretation and honest limits

- **Absence is not proof of safety:** a clean examination reducing but not eliminating the possibility of covert surveillance, so it is never presented as a guarantee the phone is clean (§4): the crucial honesty.
- **Avoid false alarm too:** ordinary or benign features not misread as surveillance, so a person is neither falsely reassured nor needlessly frightened (guide 100): the balanced honesty.
- **Distinguish the vectors:** a legitimate feature being misused distinguished from installed malware, since the response differs, so the finding is precise about what is happening (§3): the precise finding.
- **Attribute with care:** who installed or controls the surveillance addressed with care and corroboration, since it bears on serious allegations (guide 105): the careful attribution.
- **State confidence and limits:** what was found, what could not be excluded, and the limits of detection expressed at honest confidence, for both safety and evidence (guide 100): the honest compromise account.

§ 0 7 · DEPLOYMENT

Deployment: protecting the person, then the evidence

- **Making the person safer:** the first goal, identifying and, when safe to do so, closing the surveillance (a shared-location setting, a controlled account, stalkerware), so the person is protected (§5): the safety outcome.
- **Evidencing the surveillance:** the surveillance evidenced for proceedings, protective orders, family proceedings, criminal complaints, so the harm is proved (guide 98): the evidence of abuse.
- **Evidencing control and access:** the misuse of accounts and features evidenced, so coercive control and unauthorised access are shown (guides 158, 152): the control evidenced.
- **Supporting protective steps:** the findings supporting protective orders and safety planning, so the legal and safeguarding response is informed (guide 100): the protection supported.
- **Safety-led, honest presentation:** the work led by the person's safety, precise about the vector, honest about detection limits, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 20): the compromise evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: covert surveillance leaves traces across the phone and, crucially, the account and the wider setup, so detection and evidence draw on all of them, while safety governs the order and manner of every step. The phone holds the settings, apps and traces of monitoring, within iOS's inspection limits. But the iCloud account (guide 158) holds the sharing settings, associated devices and sign-in records that reveal a controlled account or misused Find My, often the real mechanism; the account's device list reveals devices the abuser has linked; the paired devices and family-sharing setup show the wider arrangement; and physical tracking devices and the abuser's own devices are adjacent sources where lawful and safe to consider. The discipline is to examine the phone, the account and the setup together for the mechanism of surveillance, most often a misused feature or controlled account rather than malware, while at every step weighing the effect on the person's safety and not alerting the perpetrator. When the phone appears clean, the account or sharing settings may hold the surveillance; when a feature is misused, the account records evidence it; and the whole picture, assembled safely, both protects the person and proves the abuse.

EVIDENCE	THE PHONE	ICLOUD ACCOUNT	SHARING / FAMILY SETUP	PAIRED / LINKED DEVICES	PHYSICAL / NETWORK	SAFETY CONSIDERATION
Stalkerware	Traces (limited)	Install via account	n/a	n/a	n/a	Do not alert on removal
Misused Find My / location	Settings	Y: sharing records	Y: who shares	Linked devices	n/a	Closing may alert
Controlled account	Signed-in account	Y: sign-ins, devices	Family organiser	Y: abuser's devices	n/a	Account change may alert
Spyware (rare)	Hard to detect	Some indicators	n/a	n/a	Network signs	Specialist, careful handling
Physical tracker	n/a	Find My items	n/a	Tracker device	Y: the device	Physical safety

Fallback strategy in one line: examine the phone, account and sharing setup together for the mechanism, usually a misused feature or controlled account, while every step is weighed for the person's safety and chosen not to alert the perpetrator.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE "SPYWARE" THAT WAS A SHARED LOCATION

A client was certain their phone had been hacked, because their abusive ex always knew where they were. The §4 settings-first discipline found the real mechanism: not malware, but §3 shared location and a Find My arrangement the ex had set up and still controlled, and a §3 partly-controlled account (guide 158). This was surveillance without any "hacking" at all. Per §5, the findings were preserved and the closing of the sharing was planned, with safeguarding, so as not to §5 alert the ex and escalate risk, and a §5 safe device was used meanwhile. The §7 misuse was evidenced for protective proceedings. The lesson is §3's: the most common covert surveillance is not malware but the misuse of legitimate features, shared location, Find My, controlled accounts, so these are checked first, and where they are the mechanism, the finding is preserved and any change planned carefully with safety in mind, because closing the surveillance can itself alert the perpetrator.

EXAMPLE 2 · SAFETY BEFORE THE SCAN

A client wanted their phone examined immediately for stalkerware. The §5 duty of care shaped the approach before any scan: because a hasty examination or removal could §5 alert a dangerous perpetrator and escalate risk, the work was coordinated with §5 safeguarding and a safety plan, the evidence §5 preserved first, and steps timed so the person was protected, not endangered, by the investigation. Only within that safety-led plan was the phone examined. The §7 person's safety came before the evidence-gathering, and the evidence was still obtained, safely. The lesson is §5's: this work carries a paramount duty of care, because handling a suspected-stalkerware phone wrongly can alert the perpetrator and escalate danger, so victim safety comes before evidence-gathering, every step is weighed for its effect on the person, and the technical work is coordinated with safeguarding rather than rushed.

EXAMPLE 3 · THE CLEAN SCAN THAT WAS NOT A GUARANTEE

An examination of a device found no stalkerware and no misused features. The §6 honesty discipline governed how this was reported: a clean result on a §4 locked-down platform reduces but does not eliminate the possibility of covert surveillance, so it was presented as reassuring but not a §6 guarantee that the phone was clean, and the §4 limits of detection stated plainly. Equally, benign features were not §6 misread as surveillance to manufacture a false alarm. The honest, balanced position, neither false reassurance nor false alarm, was given. The lesson is §6's: detection on iOS is genuinely limited, so absence of findings is not proof of safety and is never presented as a guarantee, while ordinary features are not misread as surveillance either, so the account is honest in both directions, giving the person a truthful picture on which to make safety decisions.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Rushing to scan, ignoring safety:** the gravest error, examining or cleaning the phone in a way that alerts the perpetrator and escalates danger (Example 2, §5).
- **Assuming malware, missing misused features:** looking for spyware and overlooking the far more common shared-location, Find My and account abuse (Example 1, §3).
- **Presenting a clean scan as a guarantee:** treating absence of findings as proof the phone is safe (Example 3, §6).
- **False alarm:** misreading benign features as surveillance and frightening the person needlessly (§6).
- **Removing surveillance without preserving:** destroying the evidence, and possibly alerting the abuser, by cleaning first (§5).
- **Ignoring the account:** examining the phone but not the controlled account that is the real mechanism (§4, guide 158).
- **Working in isolation:** not coordinating with safeguarding and support (§5).
- **Overstating attribution:** asserting who is responsible without care and corroboration (§6, guide 105).

Technical limitations

- **Detection is genuinely limited:** iOS's locked-down nature limits inspection, so a clean result is not conclusive: the core limit (§4).
- **Sophisticated spyware may evade detection:** advanced tools can be very hard or impossible to find (§3).
- **Misuse leaves few malware traces:** feature abuse is not malware, so it is found in settings and accounts, not scans (§3).
- **Attribution is hard:** tying surveillance to a person needs care and corroboration (§6).
- **The landscape evolves:** tools and features change, so the approach is current-aware (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

These questions are asked with care and, where there is a safety risk, in a safe setting and coordinated with safeguarding, so that asking them does not itself increase risk.

Ask your client

- Do you feel safe, and is it safe to examine this phone now, or should we plan first with safeguarding and use a safe device?
- Does someone always seem to know your location or your messages, and did anyone set up or control your Apple account or sharing?
- Who had physical access to your phone and might know your passcode?

Ask the other side / in proceedings

- Please disclose any location-sharing, Find My, family-sharing or account arrangements involving the applicant's device, and any monitoring software installed.
- Please confirm all devices and accounts with access to the applicant's data.
- Please preserve the relevant account and device records.

Ask your eDiscovery / forensic provider

- How do we examine this safely, without alerting a perpetrator or escalating risk?
- What surveillance can and cannot be detected, and how are the limits stated?
- Is the mechanism malware, a misused feature or a controlled account, and how is it evidenced and safely closed?

SUGGESTED WORDING · INSTRUCTION FOR A SUSPECTED-COMPROMISE ANALYSIS

> "We instruct you to assess the device at Schedule 1 for covert surveillance, treating the safety of the person at risk as the paramount consideration. Please: (1) before any examination, agree a safety-led plan, coordinated with safeguarding, that avoids alerting any perpetrator and, where risk is high, uses a separate safe device for communications; (2) check first the legitimate features most commonly misused, shared location, Find My, family-sharing and account control, then examine the device for stalkerware and other monitoring within the platform's limits, and review the account's devices, sign-ins and sharing; (3) preserve evidence of any surveillance before anything is removed, and plan any removal for safety, not reflexively; (4) state honestly what was and was not found, that a clean result is not a guarantee given detection limits, and that benign features are not surveillance, avoiding both false reassurance and false alarm; and (5) distinguish the mechanism precisely (misused feature, controlled account or malware), attribute with care and corroboration, and present findings to support protection and proceedings at honest confidence."

§ 12 · QUICK CONTROL

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

The suspected-compromise checklist

- ☐ Person's safety assessed; safety-led plan agreed first
- ☐ Steps chosen not to alert any perpetrator
- ☐ Safe device used for communications where risk is high
- ☐ Legitimate misused features (location, Find My, account) checked first
- ☐ Device examined for stalkerware within platform limits
- ☐ Account devices, sign-ins and sharing reviewed
- ☐ Surveillance preserved before any removal
- ☐ Clean result reported as not a guarantee; no false alarm
- ☐ Mechanism distinguished; attribution careful
- ☐ Coordinated with safeguarding; findings support protection

Red flags

- A phone scanned or cleaned before safety is considered: Example 2.
- Malware assumed while misused features are overlooked: Example 1.
- A clean scan presented as a guarantee of safety: Example 3.
- Benign features misread as surveillance.
- Surveillance removed without preserving the evidence.
- The controlled account not examined.
- Work done in isolation from safeguarding.

When to involve a digital forensic expert

Whenever a person fears their phone is being used to watch them, and always in a way that puts their safety first, because this is the one situation where the wrong technical step can cause real harm: the expert leads with safety, agreeing a plan coordinated with safeguarding that avoids alerting any perpetrator and, where risk is high, uses a safe device, before any examination (Example 2, §5). The most common mechanisms, misused shared location, Find My, family-sharing and controlled accounts, are checked first, since they are not malware at all, alongside a stalkerware examination within the platform's limits and a review of the account's devices and sign-ins (Example 1, §3, §4). Evidence is preserved before anything is removed, findings are reported honestly, a clean result is not a guarantee, and benign features are not surveillance (Example 3, §6), the mechanism is distinguished precisely and attributed with care, and the work supports protection and proceedings under CPR Part 35 or CrimPR Part 19. This guide closes the core of the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, suspected-compromise work treats the phone as the weapon and the person as the priority,

protecting them first and gathering the evidence second, with the honesty about detection's limits that their safety and the court both require.

§ 13 · COMMON QUESTIONS

Frequently asked questions

My client thinks their phone is being tracked. Where do we start?

With their safety, before any examination (§5, Example 2). If there is a risk of harm, the first step is a safety-led plan, coordinated with safeguarding, that avoids alerting the person doing the tracking, because a hasty scan or clean-up can escalate danger. Where risk is high, a separate safe device is used for communications. Only within that plan is the phone examined, checking first the legitimate features most often misused. Safety comes before evidence throughout; the evidence can still be gathered, but never at the cost of the person's safety.

Is it usually sophisticated spyware?

No, that is the rarest form (§3). By far the most common covert surveillance is consumer stalkerware installed by someone with physical access, most often an abusive partner, and, just as common and often overlooked, the misuse of legitimate features, shared location, Find My, family-sharing, or an account the abuser controls, which is not "hacking" at all. Sophisticated spyware is rare and usually the preserve of state-level actors. So the examination checks the common, mundane mechanisms first, rather than assuming an exotic one, because that is where the answer usually lies.

Why can't you just scan the phone and be sure?

Because detection on iOS is genuinely limited (§4, Example 3). iOS is a locked-down platform, which limits what monitoring software can do but also limits what an examiner can inspect, so a clean scan is reassuring but never conclusive: absence of evidence is not evidence of absence. This is stated honestly, a clean result is not presented as a guarantee that the phone is safe. At the same time, ordinary features are not misread as surveillance, so the person is given a truthful, balanced picture rather than either false reassurance or false alarm.

Should we just remove any monitoring we find?

Not reflexively, because removal can escalate risk (§5, Example 1). Cleaning a phone can alert the perpetrator that they have been discovered, which may provoke them and increase danger, and it can destroy evidence of the abuse. So any surveillance found is preserved first, and its removal is planned, timed and coordinated with safeguarding and a safety plan, with the person's safety governing when and how. Sometimes the safest course is not to remove it immediately at all. The decision is led by safety, not by the technical urge to clean the device.

Can this evidence be used in proceedings?

Yes, and it often matters greatly (§7). Evidence of covert surveillance, stalkerware, misused location-sharing, a controlled account, can support protective orders, family proceedings and criminal complaints, and can help establish coercive control and unauthorised access. It is preserved and documented properly, the mechanism distinguished precisely, and attribution handled with care and corroboration, given the seriousness of the allegations. So the work both makes the person safer and provides evidence for the legal response, presented at honest confidence, including honestly about the limits of what detection can show.

What if the abuser controls the Apple account?

That is a common and serious mechanism (§3, §4, guide 158). If the abuser set up or controls the victim's Apple account, they may have access to synced messages, photos, location and backups, and can track the person without any software on the phone at all. So the account, its associated devices, sign-ins and sharing, is reviewed as a central part of the assessment. Regaining control of the account is a key safety step, planned carefully because account changes, too, can alert the abuser, and coordinated with the wider safety plan and support.

§ 14 · REFERENCE

Glossary

Stalkerware
Consumer monitoring software installed covertly.

Spyware
Sophisticated, often state-level, surveillance software.

Misused feature
A legitimate feature used to monitor someone.

Find My
Apple's location feature, misusable for tracking.

Controlled account
An account the abuser set up or controls.

Compromise
Covert surveillance or control of a device.

Duty of care
The paramount priority of the person's safety.

No-alert principle
Acting so as not to tip off a perpetrator.

Safe device
A separate device for secure communication.

Detection limit
The point past which iOS cannot be inspected.

Sources and authoritative references

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

- cflab.uk, digital forensics services (stalkerware and compromise detection, safety-led victim-centred handling, 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 (careful, safety-aware collection and analysis 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
- Apple, device and account security, and Safety Check for situations of domestic or intimate-partner abuse: support.apple.com, Personal Safety User Guide · Coalition Against Stalkerware: stopstalkerware.org
- Forensic Science Regulator, Code of Practice v2 (careful examination and honest reporting of limits) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- Refuge tech-abuse guidance and CPR Part 35 · UK GDPR: refugetechsafety.org · justice.gov.uk, Part 35 · ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Suspected-compromise work at the laboratory treats the phone as the weapon and the person as the priority, protecting them first and gathering the evidence second. Because this work carries a paramount duty of care, it is led by the safety of the person at risk: before any examination, a safety-led plan is agreed, coordinated with safeguarding, that avoids alerting any perpetrator and, where risk is high, uses a separate safe device for communications (Example 2). The most common mechanisms are checked first, the misuse of legitimate features, shared location, Find My, family-sharing, and accounts the abuser set up or controls, since these, not malware, are usually the means, alongside an examination for stalkerware within the platform's limits and a review of the account's devices, sign-ins and sharing (Example 1, guide 158). Evidence of surveillance is preserved before anything is removed, and any removal is planned for safety rather than done reflexively. Findings are reported honestly in both directions: a clean result is not presented as a guarantee, given the genuine limits of detection on a locked-down platform, and benign features are not misread as surveillance (Example 3). The mechanism is distinguished precisely, attributed with care, and the findings support protective orders and proceedings under CPR Part 35 or CrimPR Part 19. This guide closes the core of the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is unwavering: where the phone is the weapon, the person's safety comes before the evidence, always.

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