COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Malware, Stalkerware and Compromise

The Open Platform's Larger Threat Surface, What Can Be Found, and the Duty of Care That Comes First

Android's openness, which gives it its richness for evidence, also gives it a larger threat surface than iOS. Because apps can be installed from outside the official store, stalkerware and malware are easier to install and more varied; because apps can be granted sweeping permissions, including accessibility and device-administrator rights, a monitoring app can see a great deal; and because the platform is fragmented, protections vary by device. As on iOS, the most common covert surveillance is not exotic spyware but consumer stalkerware installed by someone with physical access, or the misuse of legitimate features such as shared location, Find My Device and a controlled Google account. The consolation is that Android's openness cuts both ways: it also lets an examiner see more, so installed apps, their permissions and their behaviour can often be inspected in a way iOS does not allow. And, exactly as on iOS, this work carries a paramount duty of care, because the person whose phone is being watched may be at real risk, so their safety comes before the evidence. This guide sets out for UK lawyers how Android devices are compromised, how compromise is detected and its limits, and how a suspected-compromise case is approached safely.

⏱ 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. Android compromise work is a sensitive strand of its mobile practice: detecting stalkerware, malware and the misuse of legitimate tracking features on Android's larger threat surface, inspecting installed apps, permissions and behaviour where the platform allows, understanding the limits of detection, and, above all, handling these cases with a duty of care that puts a potential victim's safety before evidence-gathering. The analysis is safety-led and honest about its limits, and is reported under CPR Part 35 and CrimPR Part 19.

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

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: openness cuts both ways

03 How Android devices are compromised

04 Detecting compromise: what Android lets you see

05 Safety first: the duty of care

06 Interpretation and honest limits

07 Deployment: protecting the person, then the evidence

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: Android's openness gives it a larger threat surface than iOS, sideloaded stalkerware and malware are easier to install and sweeping permissions let them see a great deal, but the most common surveillance is still consumer stalkerware installed with physical access or the misuse of legitimate features, openness also lets an examiner inspect apps and permissions more fully, and, as on iOS, the person's safety comes before the evidence.

How devices are compromised (§3): sideloaded stalkerware granted accessibility, notification and administrator permissions; misused Find My Device, shared location and family features; a controlled Google account; and, rarely, sophisticated malware. **Detection (§4):** Android lets an examiner inventory apps, inspect permissions and observe behaviour more than iOS does, so more can be found, though not everything. **Safety first (§5):** the paramount duty, since mishandling can alert the perpetrator and escalate danger. **Interpretation (§6):** findings and detection limits stated honestly, without false reassurance or false alarm. **Deployment (§7):** protecting the person first, then gathering evidence, in coordination with safeguarding.

- **A larger threat surface:** sideloading and sweeping permissions make stalkerware easier.
- **Still mostly mundane:** stalkerware with physical access, or misused legitimate features.
- **Openness lets you see more:** apps, permissions and behaviour can be inspected.
- **Safety before evidence:** do not alert the perpetrator; coordinate with safeguarding.
- **Honest limits:** a clean result is not a guarantee; benign apps are not surveillance.

Figure 1 - Android's openness makes stalkerware easier to install and grant permissions, but also easier to inspect; the person's safety comes first, and detection is honest about its limits.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: openness cuts both ways

The iPhone stalkerware guide (guide 159) set out the disciplines that govern any suspected-compromise case: the phone is the weapon and the person is the target; the most common surveillance is consumer stalkerware installed by someone with physical access, or the misuse of legitimate features, not exotic spyware; detection is genuinely limited; and, above everything, the person's safety comes before the evidence, because mishandling the phone can alert the perpetrator and escalate danger. All of that applies to Android without change. What Android adds is a consequence of the openness that runs through this whole block, and it cuts both ways.

On the threat side, Android's openness makes compromise easier and more varied. Because apps can be installed from outside the official store, stalkerware and malware are simple to sideload and come in many forms, some disguised as innocuous tools (guide 167). Because Android lets apps request sweeping permissions, a monitoring app granted accessibility services, notification access, device-administrator rights or similar can read what is on the screen, capture keystrokes and notifications, track location, and resist removal, seeing far more than an iOS app could. And because the platform is fragmented, the protections against all this vary by device and version (guide 161). Alongside these sit the same mundane mechanisms as on iOS: Find My Device, shared location and family features misused to track a person, and a Google account the abuser set up or controls that gives access to synced data and the device (guide 164). On the defensive side, the same openness helps the examiner. Android exposes far more of its internals to inspection than iOS: every installed app can be inventoried from the package records, each app's permissions and special access can be read, an app's behaviour and network activity can often be observed, and sideloaded or hidden apps can be identified. So more can be found on Android than on iOS, though still not everything, and a clean result is still not a guarantee. And the duty of care is unchanged and paramount: the person in front of you may be at real risk, so the work is led by their safety, coordinated with safeguarding, and planned so that nothing alerts the person doing the watching. This guide sets out how Android devices are compromised, how compromise is detected and its limits, and how a suspected-compromise case is approached safely.

§ 0 3 · HOW DEVICES ARE COMPROMISED

How Android devices are compromised

- **Sideloaded stalkerware:** monitoring apps installed from outside the store by someone with physical access and the credential, often an abusive partner, and often disguised or hidden, the most common form (guide 167): the installed monitor.
- **Sweeping permissions:** stalkerware granted accessibility services, notification access, device-administrator or similar rights, so it can read the screen, capture notifications and keystrokes, track location and resist removal (§4): the permission-powered watcher.
- **Misused legitimate features:** Find My Device, shared location, family features and account controls used to monitor a person without any malware, very common and often overlooked (guides 168, 164): the feature abused.
- **Controlled Google account:** an account the abuser set up or controls giving access to the victim's synced messages, photos, location history and device, so the account itself is the surveillance (guide 164): the account as the tap.
- **Sophisticated malware:** advanced malware and spyware, including through malicious apps and exploits, rarer and usually targeted, considered where the threat profile warrants (guide 139): the rare, serious threat.

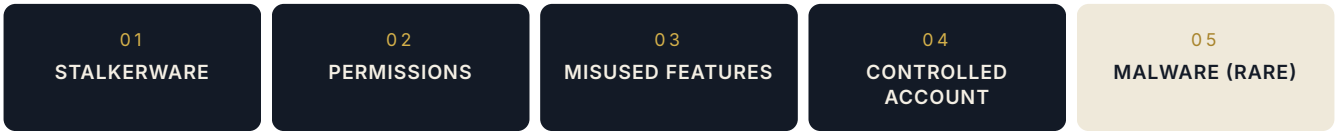

Figure 2 - how Android devices are compromised: sideloaded stalkerware empowered by sweeping permissions, misused legitimate features and controlled accounts, and rarely sophisticated malware.

§ 0 4 · DETECTING COMPROMISE

Detecting compromise: what Android lets you see

- **Check the legitimate features first:** Find My Device, location sharing, family features and Google account settings and devices checked first, since the commonest surveillance is not malware (§3): the settings review.
- **Inventory every app:** all installed apps enumerated from the package records, including hidden, disguised and sideloaded ones, and their installation source and date established (guide 167): the complete inventory.
- **Inspect permissions and special access:** each app's permissions and special access, accessibility, notification access, device administrator, usage access, examined, since stalkerware needs these and they are readable on Android (§3): the permission audit.
- **Observe behaviour where possible:** an app's behaviour, network connections and data flows observed where the platform allows, so a monitoring app's activity is evidenced rather than inferred (guide 139): the behavioural check.
- **Detection is still limited:** sophisticated or well-hidden tools, and manufacturer variation, limiting what can be found, so a clean result is reassuring but not conclusive, and stated so (§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 159): the overriding duty.
- **Do not alert the perpetrator:** the risk that examining, disabling or removing stalkerware, or changing account settings, alerts the abuser and escalates danger, so actions are chosen not to tip them off, and stalkerware may itself notify its controller of tampering (§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, never done reflexively (guide 2): the preserve-then-plan approach.
- **Coordinate with safeguarding:** the work coordinated with safeguarding, support services and, where appropriate, police, so technical steps fit a safety plan (guide 100): the coordinated response.
- **Consider a safe device:** where risk is high, a separate, safe device used 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 surveillance, so it is never presented as a guarantee the phone is clean (§4): the crucial honesty.
- **Avoid false alarm too:** legitimate apps with broad permissions (accessibility tools, parental controls the person chose, enterprise management) not misread as surveillance, so a person is neither falsely reassured nor needlessly frightened (guide 100): the balanced honesty.
- **Distinguish the vectors:** stalkerware, a misused feature and a controlled account distinguished, since the response differs (§3): the precise finding.
- **Attribute with care:** who installed or controls the surveillance addressed with care and corroboration, using installation records, account sign-ins and the wider evidence (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, a stalkerware app, so the person is protected (§5): the safety outcome.
- **Evidencing the surveillance:** the stalkerware, its permissions, its installation source and date, and its activity evidenced for protective orders, family and criminal proceedings (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 164, 168): 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 of an Android phone leaves traces across the device, the Google account and the wider setup, and Android's openness makes the device-side traces unusually visible, while safety governs the order and manner of every step. The phone holds the installed apps and their package records, permissions and special-access grants, installation sources and dates, behaviour and network traces, and the settings for location sharing and Find My Device. But the Google account (guide 164) holds the sharing settings, associated devices and sign-in records that reveal a controlled account or misused Find My Device, often the real mechanism, and its Play Store install history; the family and sharing setup shows the wider arrangement; the stalkerware's own online dashboard and provider hold what it captured and who accessed it; and physical tracking devices and the abuser's own devices are adjacent sources where lawful and safe. The discipline is to examine the phone, the account and the setup together, using Android's visibility of apps and permissions to find the mechanism, while weighing every step for the person's safety and not alerting the perpetrator. When the phone appears clean, the account or sharing settings may hold the surveillance; when stalkerware is found, its dashboard and provider evidence its use; and the whole picture, assembled safely, both protects the person and proves the abuse.

EVIDENCE	THE PHONE (APPS, PERMISSIONS)	GOOGLE ACCOUNT	SHARING / FAMILY SETUP	STALKERWARE PROVIDER / DASHBOARD	PHYSICAL / OTHER DEVICES	SAFETY CONSIDERATION
Stalkerware	Y: package, permissions, source	Install history (Play)	n/a	Y: captured data, access logs	Abuser's device	May notify on removal
Misused Find My Device / location	Settings	Y: sharing, device records	Y: who shares	n/a	Linked devices	Closing may alert
Controlled account	Signed-in account	Y: sign-ins, devices, recovery	Family manager	n/a	Abuser's devices	Account change may alert
Sophisticated malware	Harder; behaviour, network	Some indicators	n/a	n/a	Network signs	Specialist handling
Physical tracker	Tracker alerts	n/a	n/a	n/a	Y: the device	Physical safety

Fallback strategy in one line: examine the phone, account and sharing setup together, using Android's visibility of apps and permissions to find the mechanism, 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 STALKERWARE THE PERMISSIONS GAVE AWAY

A client feared their partner knew everything they did on their phone. The §4 inventory and permission audit found why: a §3 sideloaded app, disguised as a system utility and hidden from the launcher, held §3 accessibility, notification-access and device-administrator permissions it had no legitimate need for, and its §4 behaviour showed it capturing notifications and location and sending them to a remote dashboard (guide 167). Per §5, the evidence was preserved and nothing was removed until a safety plan, coordinated with safeguarding, was in place, because the app might §5 notify its controller of tampering, and a §5 safe device was used meanwhile. The §7 stalkerware, its installation date and its activity were evidenced. The lesson is §4's: Android lets an examiner inventory every app and read its permissions, so stalkerware, which needs sweeping permissions to work, is often given away by them, but its removal is planned for safety, never done reflexively.

EXAMPLE 2 · THE "SPYWARE" THAT WAS A SHARED GOOGLE ACCOUNT

A client was certain their phone had been hacked, because their ex always knew where they were. The §4 settings-first discipline found the real mechanism: not malware, but a §3 Google account the ex had set up and still controlled, signed in on the ex's own devices, with §3 Find My Device and Location History visible to them (guide 164). No app was involved. Per §5, regaining control of the account was planned with safeguarding so as not to §5 alert the ex, since an account change can itself tip off the abuser, and the §7 misuse was evidenced from the account's device and sign-in records for protective proceedings. The lesson is §3's: the most common covert surveillance is often not malware but a controlled account or misused feature, so these are checked first, and where they are the mechanism, closing them is planned carefully because the change can itself alert the perpetrator.

EXAMPLE 3 · THE BROAD PERMISSIONS THAT WERE LEGITIMATE

An examination found an app with accessibility and notification permissions, and it was tempting to report it as stalkerware. The §6 honesty discipline examined further: the app was a legitimate accessibility tool the person had chosen for a disability, its §4 installation source was the official store, and its §4 behaviour showed no capture or transmission. Reporting it as surveillance would have been a §6 false alarm, frightening the person needlessly and distracting from the real risk. Equally, the §6 clean result on the rest of the phone was reported as reassuring but not a §6 guarantee. The honest, balanced position was given. The lesson is §6's: broad permissions are necessary to stalkerware but not sufficient to prove it, since legitimate accessibility tools, parental controls and enterprise management use them too, so an app's source, purpose and behaviour are established before it is called surveillance, and neither false alarm nor false reassurance is given.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Rushing to remove, ignoring safety:** the gravest error, disabling stalkerware that notifies its controller, or changing an account, in a way that escalates danger (Examples 1 and 2, §5).
- **Assuming malware, missing the account or feature:** looking for spyware and overlooking the controlled account or shared location (Example 2, §3).
- **Reading permissions as proof:** calling a legitimate accessibility or parental app stalkerware on its permissions alone (Example 3, §6).
- **Presenting a clean scan as a guarantee:** treating absence of findings as proof the phone is safe (§6).
- **Inventorying from the launcher:** missing hidden and disguised stalkerware that only the package records reveal (§4, guide 167).
- **Removing without preserving:** destroying the evidence, and possibly alerting the abuser, by cleaning first (§5).
- **Ignoring the stalkerware's dashboard:** not pursuing the provider that holds what was captured and who accessed it (§8).
- **Working in isolation:** not coordinating with safeguarding and support (§5).

Technical limitations

- **Detection is limited:** sophisticated or well-hidden tools may evade inspection: a clean result is not conclusive (§4).
- **Permissions are necessary, not sufficient:** legitimate apps use the same permissions (§6).
- **Stalkerware may notify on tampering:** removal can itself alert the perpetrator (§5).
- **Manufacturer variation:** protections and visibility differ by device (§4).
- **The landscape evolves:** tools, disguises and features change constantly (§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 Google account, or have your phone and credential?
- Has anyone installed apps on your phone, or asked you to grant permissions?

Ask the other side / in proceedings

- Please disclose any location-sharing, Find My Device, family or account arrangements involving the applicant's device, and any monitoring app installed, with its installation source and date.
- Please confirm all devices and accounts with access to the applicant's Google account and data.
- Please preserve the relevant account, device and any monitoring-service records.

Ask your eDiscovery / forensic provider

- How do we examine this safely, without alerting a perpetrator or triggering stalkerware's tamper notifications?
- What do the app inventory, permissions and behaviour show, and what can and cannot be detected?
- Is the mechanism stalkerware, a misused feature or a controlled account, and how is it evidenced and safely closed?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID SUSPECTED-COMPROMISE ANALYSIS

> "We instruct you to assess the Android 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, accounts for stalkerware that may notify its controller of tampering, and, where risk is high, uses a separate safe device for communications; (2) check first the legitimate features and account most commonly misused, Find My Device, location sharing, family features and Google account control, devices and sign-ins; (3) inventory every installed app from the package records, including hidden, disguised and sideloaded ones, with installation source and date, audit each app's permissions and special access, and observe behaviour and network activity where the platform allows; (4) preserve evidence of any surveillance before anything is removed, and plan any removal or account change for safety; (5) establish an app's source, purpose and behaviour before calling it surveillance, avoiding both false alarm and false reassurance, and state that a clean result is not a guarantee; and (6) distinguish the mechanism precisely, attribute with care and corroboration, pursue the stalkerware's provider and dashboard where relevant, 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 Android suspected-compromise checklist

- ☐ Person's safety assessed; safety-led plan agreed first
- ☐ Steps chosen not to alert a perpetrator; tamper notifications considered
- ☐ Safe device used for communications where risk is high
- ☐ Legitimate features and account control checked first
- ☐ Every app inventoried from package records, with source and date
- ☐ Permissions and special access audited; behaviour observed
- ☐ App source, purpose and behaviour established before calling it surveillance
- ☐ Surveillance preserved before any removal or account change
- ☐ Clean result reported as not a guarantee; no false alarm
- ☐ Mechanism distinguished; attribution careful; provider/dashboard pursued

Red flags

- Stalkerware removed or an account changed before safety is planned: Examples 1 and 2.
- Malware assumed while a controlled account or shared location is overlooked: Example 2.
- A legitimate app called stalkerware on permissions alone: Example 3.
- A clean scan presented as a guarantee.
- Apps inventoried from the launcher, missing hidden ones.
- Surveillance removed without preserving the evidence.
- Work done in isolation from safeguarding.

When to involve a digital forensic expert

Whenever a person fears their Android phone is being used to watch them, and always in a way that puts their safety first, because the wrong technical step can cause real harm: the expert leads with safety, agreeing a plan coordinated with safeguarding that avoids alerting any perpetrator, accounts for stalkerware's tamper notifications, and uses a safe device where risk is high, before any examination (§5). The commonest mechanisms, a controlled Google account and misused Find My Device or location sharing, are checked first (Example 2, §3), and Android's openness is then used to inventory every app from the package records, audit permissions and special access, and observe behaviour, so stalkerware is often given away by the permissions it needs (Example 1, §4), while an app's source, purpose and behaviour are established before it is called surveillance, so no false alarm is raised and no false reassurance given (Example 3, §6). Evidence is preserved before anything is removed, the mechanism is distinguished and attributed with care, the stalkerware's provider is pursued where relevant, and findings support protection and proceedings under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, Android compromise work

uses the platform's openness to see what is watching, treats the person as the priority, and gathers the evidence second, with the honesty about detection's limits that their safety and the court both require.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is Android more vulnerable to stalkerware than iPhone?

Its threat surface is larger, and its visibility is greater (§2). Because apps can be sideloaded and granted sweeping permissions, accessibility, notification access, device-administrator rights, stalkerware is easier to install on Android and can see more once installed. But the same openness lets an examiner inventory every app, read its permissions and observe its behaviour in ways iOS does not allow, so more can be found. And on both platforms the commonest surveillance is not exotic spyware but stalkerware installed with physical access or a misused account or feature, and the duty of care is identical.

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

With their safety, before any examination (§5). 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 removal or account change can escalate danger, and some stalkerware notifies its controller of tampering. Where risk is high, a separate safe device is used. Only within that plan is the phone examined, starting with the legitimate features and account controls most often misused. Safety comes before evidence throughout.

How can stalkerware be found on Android?

Often through the permissions it needs (§4, Example 1). Stalkerware must be granted accessibility services, notification access, device-administrator or similar rights to read the screen, capture notifications and track location, and on Android those grants are readable. So every app is inventoried from the package records, including hidden and disguised ones, with its installation source and date; each app's permissions and special access are audited; and behaviour and network activity are observed where possible. Sophisticated or well-hidden tools may still evade this, so a clean result is reassuring but not a guarantee.

Does an app with broad permissions prove it is spyware?

No, permissions are necessary but not sufficient (§6, Example 3). Legitimate accessibility tools, parental controls a person chose, and enterprise management all use the same sweeping permissions, so calling an app stalkerware on its permissions alone risks a false alarm that frightens the person and distracts from the real risk. An app's installation source, its purpose and its actual behaviour, whether it captures and transmits data, are established before it is called surveillance, so the person receives neither false alarm nor false reassurance.

What if the abuser controls the Google account?

That is a common and serious mechanism (§3, Example 2, guide 164). If the abuser set up or controls the victim's Google account, they may see synced messages, photos, Location History and Find My Device, and can track the person without any app on the phone at all. So the account's devices, sign-ins, recovery settings and sharing are reviewed as a central part of the assessment. Regaining control of the account is a key safety step, planned carefully with safeguarding because an account change can itself alert the abuser.

Should we just uninstall any stalkerware we find?

Not reflexively, because removal can escalate risk (§5, Example 1). Many stalkerware apps notify their controller when they are disabled or removed, so uninstalling one can tell the perpetrator they have been discovered and provoke them, 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.

§ 14 · REFERENCE

Glossary

Stalkerware
Consumer monitoring software installed covertly.

Sideloading
Installing an app from outside the official store.

Accessibility services
A permission letting an app read the screen and input.

Notification access
A permission letting an app read notifications.

Device administrator
A right letting an app resist removal and control the device.

Find My Device
Google's location feature, misusable for tracking.

Controlled account
A Google account the abuser set up or controls.

Tamper notification
Stalkerware alerting its controller to removal.

Package records
The system's list of every installed app.

Safe device
A separate device for secure communication.

Sources and authoritative references

The Android 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 (Android stalkerware and malware 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
- Google, Android safety and security (Play Protect, permissions, Find My Device) and the Coalition Against Stalkerware: support.google.com, Play Protect · stopstalkerware.org
- Refuge tech-abuse guidance; Forensic Science Regulator, Code of Practice v2; ISO/IEC 27037: refugetechsafety.org · gov.uk, FSR Code · iso.org, 27037
- CPR Part 35 · UK GDPR: justice.gov.uk, Part 35 · ico.org.uk

DISCLAIMER

This publication provides general information about Android malware, stalkerware and compromise as at September 2026. This is a safety-critical area: where a person may be at risk, their safety comes before evidence-gathering, steps must be planned to avoid alerting a perpetrator, including stalkerware that notifies its controller of tampering, and the work should be coordinated with safeguarding and support services. Detection is limited, a clean result is not a guarantee of safety, and broad permissions alone do not prove surveillance. If you or someone you are advising is in immediate danger, contact the police or a specialist support service. 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

Android compromise work at the laboratory uses the platform's openness to see what is watching, treats the person as the priority, and gathers 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, accounts for stalkerware that may notify its controller of tampering, and, where risk is high, uses a separate safe device (guide 159). The commonest mechanisms are checked first, a controlled Google account and misused Find My Device, location sharing and family features (Example 2, guides 164, 168), and Android's visibility is then used to inventory every installed app from the package records, including hidden, disguised and sideloaded ones with their installation source and date, to audit each app's permissions and special access, and to observe behaviour and network activity, so that stalkerware is often given away by the sweeping permissions it needs (Example 1, guide 167). An app's source, purpose and behaviour are established before it is called surveillance, so that a legitimate accessibility tool or parental control is not reported as stalkerware and the person receives neither false alarm nor false reassurance, with a clean result reported as reassuring but not a guarantee (Example 3). Evidence of surveillance is preserved before anything is removed, any removal or account change is planned for safety, the mechanism is distinguished and attributed with care, the stalkerware's provider and dashboard are pursued where relevant, and the findings support protective orders and proceedings under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is unwavering across both mobile blocks: 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