COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

The Google Account: Android's Cloud Estate

Location History, Photos, Backups and Activity: The Account That Often Knows More Than the Phone

Behind nearly every Android phone sits a Google account, and for many users it is where the real record lives. It holds the device's backups, the photo library, the messages and contacts that sync, the files in Drive, and, distinctively, Google's own records of the user's activity: the Location History (now Timeline) of where they went, the searches they made, the videos they watched, the places they looked up. It also records every device that has signed in. Like iCloud for the iPhone, this makes the account the richest source in many matters, and the route to evidence when a locked or constrained Android device gives up little. But it is reached only lawfully, by consent, by lawful process to Google, or by production, and Google's own controls, including the user's ability to pause, auto-delete or move data on-device, shape what survives and where. This guide sets out for UK lawyers what the Google account holds, why it so often knows more than the phone, how it is reached lawfully, and how its distinctive activity records are read honestly.

⏱ 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. Google account analysis is a central strand of its Android and cloud work: reaching, lawfully and proportionately, the backups, photos, messages, files and distinctive activity records, Location History, search and browsing activity, that the account holds, recognising it as the real store behind the device, and reading its activity records honestly. The analysis corroborates the account with the devices and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | GOOGLE ACCOUNT & TAKEOUT ANALYSIS | LOCATION HISTORY & ACTIVITY RECORDS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: behind nearly every Android phone sits a Google account that holds the device's backups, photos, messages and files and, distinctively, Google's own records of the user's activity, Location History, searches, browsing and more, so the account often knows more than the phone and is the route to evidence when a locked or constrained device gives up little, but it is reached only lawfully and shaped by the user's own controls.

What it holds (§3): device backups, Google Photos, synced messages and contacts, Drive files, and records of every device signed in. **The activity records (§4):** Location History (Timeline) of where the user went, search and browsing history, app activity and more, a distinctive record of a life. **Lawful access (§5):** by the account holder's consent (including Takeout), by lawful process to Google, or by production, never improperly. **Controls and limits (§6):** the user can pause, auto-delete or keep data on-device, so what survives, and where, must be established and read honestly. **Deployment (§7):** the account as a first-class source and as fallback when the device is sealed, corroborated and read with care.

- **The account knows more:** often the real store behind the Android phone.
- **Distinctive activity records:** Location History, searches and browsing, a record of a life.
- **The route around a sealed device:** reachable regardless of the phone's lock.
- **Reached only lawfully:** consent, lawful process to Google, or production.
- **User controls shape it:** pause, auto-delete and on-device storage change what survives.

Figure 1 - the Google account behind an Android phone holds its backups, photos and files plus distinctive activity records, reachable lawfully regardless of the phone's lock and shaped by the user's own controls.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the account that knows more

The iPhone block explained that for many Apple users the device is only a window and the iCloud account behind it is the real store (guide 158). Android has its exact counterpart, and in one respect it goes further. Behind nearly every Android phone sits a Google account, signed in at setup and running through everything the phone does. It holds the phone's backups, the Google Photos library, the messages and contacts that sync, the files in Google Drive, and a record of every device that has ever signed in. That much mirrors iCloud. What is distinctive about the Google account is that Google also keeps its own records of what the user did with its services: the Location History, now called Timeline, of where the user went day by day; the searches they typed; the web pages they visited in Chrome; the videos they watched; the places they looked up in Maps; the apps they used. For a user who has left these on, and many do, the account is not merely a backup of the phone but a running diary of a life, kept by Google.

For the lawyer this has two consequences. First, the account is often the richest source in an Android matter, richer than the phone, because it aggregates all the user's devices, holds more and older data, and adds the activity records the phone alone does not keep in that form. Second, it is the route around a sealed device: a locked, encrypted or constrained Android phone (guides 162, 163) may give up little, but the Google account behind it is reachable lawfully regardless of the phone's lock, and frequently holds most of what the phone would have. Two cautions temper this. The account is reached only lawfully, by the account holder's consent, including through Google's own Takeout export, by lawful process served on Google, or by production in disclosure, and never by improper access. And Google gives users real control over these records: they can pause Location History and activity tracking, set data to auto-delete after a period, delete it manually, or keep Timeline data only on the device rather than in the cloud, so what actually survives, and where, must be established for each account and read honestly rather than assumed. This guide sets out what the Google account holds, its distinctive activity records, how it is reached lawfully, how user controls and retention shape it, and how it is deployed as source and fallback.

§ 0 3 · WHAT THE ACCOUNT HOLDS

What the Google account holds

- **Device backups:** Android backups of the device's settings, app data and (for many) messages and call logs, held in the account, so a device's contents can be reconstructed from the cloud (guide 147): the cloud backup.
- **Google Photos:** the photo and video library synced to the account, often the complete library with metadata, so the user's images are held centrally (guide 149): the photo store.
- **Messages, contacts and calendar:** contacts and calendar synced, and messages backed up or synced where enabled, so communication and personal data reach the cloud (guides 148, 153): the synced PIM.
- **Drive and documents:** files, documents and downloads in Google Drive, so the user's documents are held in the account (guide 135): the file store.
- **Devices and sign-ins:** the account's record of every device signed in, with activity and security events, so all associated devices and access to the account are evidenced (guide 158): the account inventory.

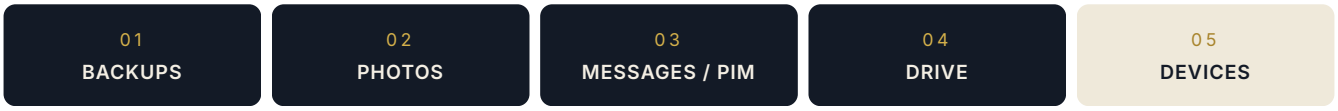

Figure 2 - the Google account holds device backups, the photo library, synced messages and personal data, Drive files, and the record of every device signed in.

§ 0 4 · THE ACTIVITY RECORDS

The distinctive activity records

- **Location History (Timeline):** Google's record of where the user went, day by day, with places and journeys, a rich location record where it is on, though increasingly stored on-device rather than in the cloud (guide 152): the where-they-went record.
- **Search and browsing activity:** the searches typed and the pages visited in Chrome, synced to the account, revealing intent, research and interest (guide 136): the what-they-looked-for record.
- **App, video and Maps activity:** apps used, videos watched and places looked up in Maps, recorded as activity, filling out the picture of interest and movement (guide 151): the what-they-did record.
- **Timestamped and revealing:** the records timestamped and often detailed, so they place actions in time and can corroborate or contradict an account, read with care about what they show (guide 100): the dated activity.
- **Subject to user control:** each record able to be paused, auto-deleted or deleted by the user, so its presence and completeness depend on the user's settings (§6): the controllable record.

§ 0 5 · REACHING THE ACCOUNT LAWFULLY

Reaching the account lawfully

- **By consent, including Takeout:** the account holder's consent providing access, including through Google Takeout, which exports the account's data in bulk, the cleanest route (guides 117, 20): the consent and export route.
- **By lawful process to Google:** lawful process served on Google compelling production of account data Google can provide, subject to Google's policies and the applicable legal framework (guides 111 to 114): the legal-process route.
- **By production in disclosure:** a party required to disclose relevant Google account data as part of their disclosure, producing their own account records (guides 5, 6): the disclosure route.
- **Never improper access:** the account never accessed by guessing credentials or unauthorised sign-in, which would be unlawful and inadmissible (guide 117): the lawful boundary.
- **Proportionate and scoped:** the collection scoped to the categories and period the matter requires and minimised, given the breadth and sensitivity, especially of location and activity records (guide 20): the proportionate collection.

§ 0 6 · CONTROLS, RETENTION AND LIMITS

User controls, retention and honest limits

- **Pausing and deletion:** the user able to pause Location History and activity tracking and to delete records manually, so a paused or deleted record is simply absent, an honest limit (§4): the user's switch.
- **Auto-delete:** auto-delete settings removing records after a chosen period, so older activity may be gone by design, and the retention setting is established (guide 134's rotation theme): the automatic pruning.
- **On-device Timeline:** Timeline data increasingly stored on the device rather than in the cloud, so the device, not the account, may hold the location record, and vice versa depending on settings and version (guide 152): the where-is-it question.
- **Establish the settings:** the account's settings and retention established early, so what survives and where is known before expectations are set (guide 161): the settings check.
- **Read honestly:** an absent or partial record read as the product of settings or deletion, not as proof of inactivity, and the activity records read for what they show, at honest confidence (guide 100): the honest reading.

§ 0 7 · DEPLOYMENT

Deployment: the account as source and fallback

- **The account as primary source:** the Google account used as a first-class, often primary, source, aggregating devices and adding activity records the phone lacks (§2): the account as source.
- **The route around a sealed device:** the account reached lawfully when the phone is locked, encrypted or constrained, supplying most of what it would have (guides 162, 163): the account as fallback.
- **Movement from Location History:** Timeline placing the user's movements over a period, corroborated with the phone and other sources, so travel and presence are evidenced (guide 152): the movements traced.
- **Intent from search and browsing:** search and browsing records evidencing research, intent and interest, read with care about inference (guide 136): the intent evidenced.
- **Lawful, proportionate, honest presentation:** the account data obtained lawfully, scoped proportionately, its settings and retention accounted for, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 20): the account evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the Google account is the hub of the Android estate, and it both aggregates the devices and adds records they do not hold in the same form. The account holds backups, photos, synced messages and PIM, Drive files, device records and the activity records. But the devices (guides 161 to 163) hold local data, including Timeline data that, under current settings, may live on-device rather than in the cloud; the manufacturer's cloud (Samsung Cloud and equivalents) holds its own backups and synced data; local backups hold device contents; a paired wearable holds shared health and location data; the counterparts hold their side of communications; and the app providers and carriers hold records. The discipline is to treat the account as the real store and often the primary source, reached lawfully, while establishing where each record actually lives, since a user's settings can move Timeline on-device, pause activity or auto-delete it, and to corroborate the account with the devices and the wider estate. When the phone is sealed, the account supplies most of what it would; when the cloud record is paused or deleted, the device or manufacturer cloud may hold it; and when the account's activity records exist, they corroborate and enrich everything else.

EVIDENCE	GOOGLE ACCOUNT	ANDROID DEVICE	MANUFACTURER CLOUD	BACKUPS (LOCAL/ CLOUD)	PAIRED / COUNTERPART	PROVIDER / CARRIER
Photos	Y: Google Photos	Y: local	Y: gallery sync	Y	Shared copies	n/a
Messages	Y: if backed up/synced	Y: at depth	Y: if backed up	Y	Y: counterpart	Provider metadata
Location History	Y: if cloud Timeline on	Y: on-device Timeline	Some	Some	Wearable	Carrier cell (area)
Search / browsing	Y: activity records	Y: Chrome local	n/a	Some	n/a	n/a
Devices / sign-ins	Y: account record	n/a	Some	n/a	n/a	n/a

Fallback strategy in one line: treat the account as the real store, reached lawfully, establish where each record actually lives given the user's settings, and corroborate it with the device and estate; when the phone is sealed, the account supplies most of what it would.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE SEALED PHONE AND THE ACCOUNT THAT KNEW EVERYTHING

A modern Android phone was locked and encrypted, and §7 gave up nothing without the credential (guide 163). The §7 account was the route: reached §5 lawfully by production, the Google account held the device's backups, the Google Photos library, synced messages and contacts, and the §4 activity records, Timeline, searches and browsing. Together these supplied most of what the sealed phone would have, and more, since the §4 activity records existed in a form the phone did not hold. The §6 settings were checked and the data collected proportionately. The vault stayed shut, but the account knew everything. The lesson is §2's and §7's: the Google account is the route around a sealed or constrained Android device, reachable lawfully regardless of the phone's lock and frequently holding most of what the phone would have, together with activity records the phone does not keep in the same form.

EXAMPLE 2 · THE TIMELINE THAT PLACED THE JOURNEY

A matter turned on where a person had been over several days. The §4 Location History in their Google account, obtained §5 lawfully, recorded their movements day by day, the places visited and the journeys between them (guide 152). Per §7, this was corroborated with the phone's own location data and with a paired wearable, and the §6 accuracy and settings were established, so the placement rested on convergence and was read at honest confidence. The account's diary of movement answered the question. The lesson is §4's: Location History is a distinctive and often detailed record of where a user went, and, obtained lawfully and corroborated with the device and other sources, it can place a person's movements over a period, provided its settings and accuracy are established and it is read honestly.

EXAMPLE 3 · THE RECORD THAT WAS ABSENT BY THE USER'S CHOICE

An expected Location History record was absent, and a party argued the absence proved the person had not travelled. The §6 controls discipline corrected the inference: the account's settings showed Location History had been paused and auto-delete set to a short period, and Timeline data was stored on-device rather than in the cloud, so the cloud record was absent by the user's settings, not because no travel occurred. The §8 device's on-device Timeline and the manufacturer cloud were pursued instead, and the §6 absence read honestly. The silence was a setting, not a fact. The lesson is §6's: Google gives users real control, to pause, auto-delete, delete or keep data on-device, so an absent record is read as the product of settings or deletion, never as proof of inactivity, and the account's settings are established early so that the enquiry looks where the record actually lives.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating the phone as the only source:** the cardinal error, examining the device and forgetting the account that knows more (§2).
- **Giving up on a sealed phone:** not reaching the account that is available regardless of the lock (Example 1, §7).
- **Improper access:** reaching the account by guessing credentials rather than lawfully (§5).
- **Reading absence as inactivity:** treating a paused, deleted or on-device record as proof nothing happened (Example 3, §6).
- **Not checking the settings:** assuming the cloud holds Timeline or activity when the user's settings moved or removed it (§6).
- **Over-collecting:** taking the whole account, including intimate activity records, without scoping (§5, guide 20).
- **Overreading activity records:** inferring intent or presence from searches or Timeline without corroboration (Example 2, §7).
- **Ignoring the device records:** not using the account's device list to find further sources (§3).

Technical limitations

- **Access is lawful only:** consent, process or production, never improper (§5).
- **User controls govern survival:** pause, auto-delete and on-device storage decide what exists and where (§6).
- **Google's policies bound process:** what Google provides depends on its policies and the legal framework (§5).
- **Records are not proof of presence:** an account's activity attributes to the account, and to a person with care (§7).
- **Google evolves constantly:** what is kept, where and for how long changes over time (§4, §6).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the Google account likely to hold the relevant data, especially if the phone is locked or constrained?
- Is the account holder's consent (and a Takeout export) available, or is lawful process to Google or production the route?
- What are the account's Location History and activity settings, retention and on-device options, so we know what survives and where?

Ask your opponent

- Please preserve and disclose, proportionately, the relevant data from the Google account at Schedule 1, including backups, Photos, synced messages and contacts, Drive files, device and sign-in records, and Location History and activity records for the relevant period.
- Please confirm the account's Location History and activity settings, any auto-delete period, and whether Timeline data is stored on-device.
- Please confirm all devices signed in to the account.

Ask your eDiscovery / forensic provider

- What does the account hold, and does it supply what a sealed or constrained phone cannot?
- How is the account reached lawfully, and how are the activity records read and corroborated?
- What do the settings and retention mean for what survives, and where does each record actually live?

SUGGESTED WORDING · INSTRUCTION FOR A GOOGLE ACCOUNT ANALYSIS

> "We instruct you to examine the Google account at Schedule 1 relevant to Schedule 2, scoped to the categories and period the matter requires. Please, obtaining access lawfully (by the account holder's consent including a Takeout export, by lawful process served on Google, or by production in disclosure) and never by improper means, and handling the data proportionately: (1) establish what the account holds, device backups, Google Photos, synced messages and contacts, Drive files, and the record of devices and sign-ins; (2) recover and analyse the activity records, Location History (Timeline), search and browsing activity, app, video and Maps activity, for the relevant period; (3) establish the account's settings, any pausing, auto-delete period, manual deletion and on-device Timeline storage, and state honestly what survives and where, reading any absent record as the product of settings rather than proof of inactivity; (4) corroborate the account data with the device, paired devices and the wider estate, and attribute activity to a person with care; and (5) use the account's device records to identify all associated devices, and present findings at honest confidence."

§ 12 · QUICK CONTROL

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

The Google account checklist

- ☐ Account treated as a first-class, often primary, source
- ☐ Access obtained lawfully (consent/Takeout, process or production)
- ☐ Backups, Photos, messages, PIM, Drive and device records recovered
- ☐ Location History and activity records recovered for the period
- ☐ Settings, retention and on-device storage established
- ☐ Absent records read as settings/deletion, not inactivity
- ☐ Activity records corroborated with device and estate
- ☐ Activity attributed to a person with care
- ☐ Collection scoped and minimised proportionately
- ☐ Findings and limits stated honestly

Red flags

- The phone treated as the only source; account forgotten: §2.
- A sealed phone treated as the end of the enquiry: Example 1.
- Account accessed improperly rather than lawfully.
- An absent Location History read as proof of no travel: Example 3.
- Settings not checked; Timeline assumed to be in the cloud.
- The whole account collected without scoping.
- Intent or presence inferred from activity without corroboration: Example 2.

When to involve a digital forensic expert

Whenever an Android matter arises, and always when the phone is locked or constrained, because the Google account behind it so often knows more than the phone: the expert treats the account as a first-class, frequently primary, source, reached lawfully by consent and Takeout, process to Google, or production, and establishes what it holds, backups, Photos, synced messages, Drive files, device records and the distinctive activity records (Example 1, §3, §4). The account's settings, retention and on-device storage are established early so that what survives, and where, is known and an absent record is read as a setting rather than as inactivity (Example 3, §6); Location History and activity records are corroborated with the device and estate and attributed with care (Example 2, §7); the collection is scoped proportionately given the intimacy of the activity data; and findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, Google account work reaches the store behind the Android phone, and the diary of a life that Google keeps alongside it, lawfully, proportionately and with a clear-eyed understanding of the user controls that shape what remains.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Why is the Google account so important in Android matters?

Because it often knows more than the phone (§2). Behind nearly every Android device, the account holds backups, the photo library, synced messages and contacts, Drive files and a record of every device signed in, like iCloud, and it adds Google's own activity records, Location History, searches, browsing, app and Maps activity, that the phone does not keep in the same form. It aggregates all the user's devices, holds more and older data, and is reachable lawfully regardless of the phone's lock. So it is frequently the richest source, and the route around a sealed device.

If the phone is locked, can the account still be reached?

Yes, and that is often the way forward (§7, Example 1). The account is reached lawfully by the account holder's consent (including a Takeout export), by lawful process served on Google, or by production in disclosure, none of which depends on unlocking the phone. A locked, encrypted or constrained device may give up little, but the account behind it frequently holds most of what the phone would have, plus the activity records. So a sealed phone does not end the enquiry; the account is pursued in parallel with any lawful route to the credential.

What is Location History, and how reliable is it?

Google's record of where the user went, now called Timeline (§4, Example 2). Where it is on, it records places visited and journeys between them, day by day, and can place a person's movements over a period with real force. Its reliability depends on its settings and accuracy, and it is corroborated with the phone's own location data and other sources so a placement rests on convergence. Increasingly, Timeline data is stored on the device rather than in the cloud, so where it actually lives is established before it is sought.

The account shows no Location History. Does that prove the person didn't travel?

No, it may simply reflect the user's settings (§6, Example 3). Users can pause Location History, set it to auto-delete after a period, delete it manually, or keep Timeline data only on the device, so an absent cloud record is read as the product of settings or deletion, never as proof of inactivity. The account's settings and retention are established early, and where the cloud record is absent the device's on-device Timeline, the manufacturer's cloud and other location sources are pursued instead. Silence in the account is a setting to investigate, not a fact to rely on.

How is Google account data obtained lawfully?

By consent, lawful process or production (§5). The cleanest route is the account holder's consent, and Google Takeout lets them export their data in bulk; alternatively, lawful process can be served on Google to compel production of data it can provide, subject to its policies and the legal framework; and a party can be required to disclose their own account data. Access is never obtained by guessing credentials or unauthorised sign-in, which would be unlawful and inadmissible. Given the intimacy of activity records, the collection is scoped and minimised to what the matter requires.

Do search and browsing records prove what someone intended?

They evidence what was searched and visited, and intent is inferred with care (§4, §7). Search and browsing activity can be powerful evidence of research, interest and intent, but the inference from a search to a state of mind is made cautiously and corroborated, and the activity is attributed to the account first and to a person only with care, since accounts and devices can be shared. So these records are read for what they show, that certain searches and visits occurred at certain times, and any inference about intent is stated at honest confidence rather than assumed.

§ 14 · REFERENCE

Glossary

Google account
The account behind an Android device and Google services.

Android backup
A cloud backup of device settings and data.

Google Photos
The account's synced photo and video library.

Google Drive
The account's file storage.

Location History / Timeline
Google's record of where the user went.

Activity records
Search, browsing, app, video and Maps activity.

Google Takeout
The user's bulk export of their account data.

Auto-delete
A setting removing records after a period.

On-device Timeline
Location data kept on the phone, not the cloud.

Lawful process
A legal instrument compelling production from Google.

Sources and authoritative references

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

- cflab.uk, digital forensics services (Google account and Takeout analysis, Location History and activity records, lawful cloud access, 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 02 · Identification (lawful cloud collection and identification as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/identification
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Google, activity controls and Location History / Timeline documentation, and Google Takeout: support.google.com, Web & App Activity · support.google.com, Timeline · takeout.google.com
- Google, transparency and legal process for user data requests: support.google.com, legal process · ICO, UK GDPR guidance (sensitive location and activity data): ico.org.uk
- Forensic Science Regulator, Code of Practice v2 and ISO/IEC 27037 · PD 57AD and CPR Part 35: gov.uk, FSR Code · iso.org, 27037 · justice.gov.uk, PD 57AD · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Google account work at the laboratory reaches the store behind the Android phone, and the diary of a life that Google keeps alongside it. The account is treated as a first-class, frequently primary, source, reached only lawfully, by the account holder's consent including a Takeout export, by lawful process served on Google, or by production in disclosure, and never by improper means (guide 117). Its contents are established, device backups, the Google Photos library, synced messages and contacts, Drive files and the record of every device signed in, together with the distinctive activity records, Location History or Timeline, search and browsing, app, video and Maps activity, that the phone does not keep in the same form, so that a locked, encrypted or constrained device is no longer the end of the enquiry (Example 1, guides 162, 163). The account's settings, retention and on-device storage are established early, so that what survives and where is known, and an absent record is read as the product of pausing, auto-delete, deletion or on-device storage rather than as proof of inactivity (Example 3). The activity records are corroborated with the device, paired devices and the wider estate and attributed to a person with care (Example 2, guide 152), the collection is scoped and minimised given the intimacy of the data, and findings are reported at honest confidence 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 insight mirrors the iPhone block's: the device is often only a window, and the account behind it, reached lawfully and read with a clear understanding of the user's controls, is where the real record, and frequently the answer, is found.