COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iCloud: The Account as the Real Evidence Store

Why the Evidence Often Lives in the Account, Not the Device, and How to Reach It Lawfully

For many Apple users the device is only a window; the real store of their data is the iCloud account behind it. Photos, messages, backups of every device, files, notes, contacts, calendars, browsing, health and app data all sync to iCloud, and the account often holds more, and older, data than any single device, together with the records of every device that has ever signed in. This makes the account, not the phone, the richest source in many matters, and sometimes the only route to evidence when a device is lost, wiped, locked or destroyed. But reaching it is a legal exercise as much as a technical one. iCloud data is obtained lawfully, by the account holder's consent, by lawful process to Apple, or by production, and Advanced Data Protection, Apple's optional end-to-end encryption for much iCloud data, changes what even Apple can provide. This guide sets out for UK lawyers what iCloud holds, why the account is so often the real evidence store, how it is reached lawfully, and how Advanced Data Protection changes the picture.

⏱ 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. iCloud and account analysis is a central strand of its cloud and mobile work: reaching, lawfully and proportionately, the photos, messages, backups, files and app data an account holds, recognising the account as the real evidence store, and understanding how Advanced Data Protection changes what can be obtained. The analysis treats the account as a first-class source, corroborates it with the devices, and is reported under CPR Part 35 and CrimPR Part 19, with lawful access and proportionality observed throughout.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ICLOUD & ACCOUNT FORENSICS | LAWFUL ACCESS & ADP AWARENESS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: for many Apple users the device is only a window and the real store of their data is the iCloud account behind it, which holds photos, messages, backups of every device, files and app data, often more and older than any device, making the account the richest source in many matters and sometimes the only route when a device is gone, but reachable only lawfully.

What it holds (§3): photos, messages, device backups, files, notes, contacts, calendars, browsing, health and app data, plus records of every device that has signed in. **The real store (§4):** the account often holds more and older data than any single device, and survives the loss, wiping or locking of a device. **Lawful access (§5):** iCloud is reached only lawfully, by the account holder's consent, by lawful process to Apple, or by production, never by improper access. **Advanced Data Protection (§6):** Apple's optional end-to-end encryption for much iCloud data changes what even Apple can provide, so its status is established. **Deployment (§7):** using the account as a first-class source and as fallback when devices are unavailable, lawfully and proportionately.

- **The account behind the device:** the device is a window; the account is the store.
- **More and older data:** the account often holds what no single device does.
- **Survives lost devices:** the route to evidence when a device is wiped, locked or gone.
- **Reached only lawfully:** by consent, lawful process to Apple, or production.
- **ADP changes the picture:** end-to-end encryption limits what even Apple can provide.

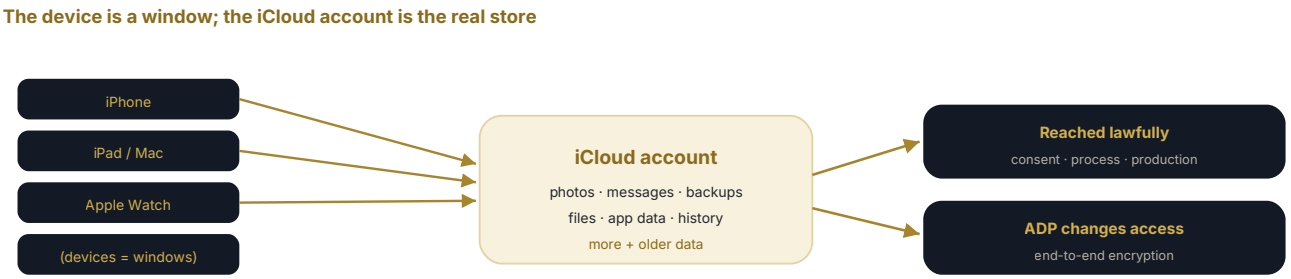

Figure 1 - devices are windows onto the iCloud account, which holds more and older data than any one of them, reachable only lawfully and shaped by whether Advanced Data Protection is enabled.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the account behind the device

It is natural to think of the evidence as living on the phone. For many Apple users, that is only half true, and often the less important half. Behind every iPhone, iPad, Mac and Watch sits an iCloud account, and for a user who has embraced Apple's ecosystem, that account is the real store of their digital life. Photos sync to iCloud Photos; messages sync to Messages in iCloud; every device backs up to iCloud; files, notes, contacts, calendars, browsing history, health data and the data of countless apps all sync to the account. The device in the hand is, in a real sense, just a window onto this account, showing a current view of data whose master copy, and whole history, lives in the cloud. And the account keeps more than any single device: it retains data the device has offloaded, backups of devices long since replaced, and a record of every device that has ever signed in to it.

For the lawyer this reframes where the evidence is. In many matters the iCloud account, not the phone, is the richest single source, because it aggregates the data of all the user's devices and often holds more, and older, material than any one of them. It is also, crucially, the route to evidence when the device itself is unavailable: a phone that is lost, wiped, locked or destroyed may have an intact iCloud account behind it, holding backups and synced data that reconstruct much of what the device held. So the account deserves to be treated as a first-class source, sometimes the primary one, not an afterthought. But reaching it is as much a legal exercise as a technical one, and this is the second theme. iCloud data belongs to the account holder and is held by Apple, so it is obtained lawfully, by the account holder's consent and credentials, by lawful process served on Apple, or by production in disclosure, never by improper or unauthorised access. And a further factor now shapes what is even possible: Advanced Data Protection, Apple's optional setting that end-to-end encrypts much iCloud data, so that even Apple cannot provide it in readable form. Whether it is enabled changes the picture entirely. The task, then, is to recognise the account as the real evidence store, to understand what it holds, to reach it lawfully, and to establish how Advanced Data Protection affects access. This guide sets out how.

§ 0 3 · WHAT ICLOUD HOLDS

What iCloud holds

- **Photos and messages:** iCloud Photos and Messages in iCloud holding the account's photos and conversations, often the whole library and history, synced across devices (guides 149, 148): the synced content.
- **Device backups:** iCloud backups of the user's devices, each a rich snapshot of a device's data, including of devices no longer in use (guide 147): the device backups.
- **Files, notes and PIM:** iCloud Drive files, notes, contacts, calendars and reminders synced to the account, so documents and personal information are held centrally (guide 135): the files and PIM.
- **App, health and browsing data:** app data, health data and browsing history synced to iCloud where enabled (guides 150, 136), so much of a device's activity is mirrored in the account: the wider synced data.
- **Account and device records:** the account's own records, sign-ins, the devices associated with it, and activity, so who accessed it and from what is evidenced (guide 111): the account metadata.

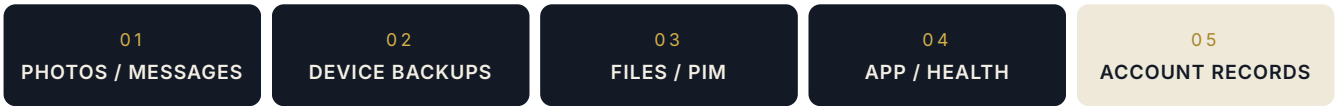

Figure 2 - iCloud holds photos, messages, device backups, files, personal information and app and health data, plus the account's own sign-in and device records.

§ 0 4 · THE REAL EVIDENCE STORE

Why the account is the real evidence store

- **Aggregates all devices:** the account holding the data of all the user's devices together, so it is a single, comprehensive source where a device is only one window (guide 130): the aggregated source.
- **More and older data:** the account retaining offloaded data, old device backups and history the current device no longer holds, so it often has more, and older, material (guide 147): the deeper record.
- **Survives the device:** the account persisting when a device is lost, wiped, locked or destroyed, so it is the route to evidence the device can no longer give (guide 130): the fallback route.
- **Records of every device:** the account holding records of every device that has signed in, so devices unknown or undisclosed can be identified (guide 111): the device inventory.
- **Corroborates the devices:** the account corroborating and completing what the devices show, so a finding rests on both device and account (guide 130): the corroborating store.

§ 0 5 · REACHING ICLOUD LAWFULLY

Reaching iCloud lawfully

- **By consent and credentials:** the account holder's informed consent and credentials providing lawful access, the cleanest route where available (guides 117, 20): the consent route.
- **By lawful process to Apple:** lawful process (a court order or the appropriate legal instrument) served on Apple compelling production of account data Apple can provide (guides 111 to 114): the legal-process route.
- **By production in disclosure:** the account holder required to disclose relevant iCloud data as part of their disclosure obligations, so a party produces their own account data (guides 5, 6): the disclosure route.
- **Never improper access:** access never obtained by guessing credentials, unauthorised sign-in or other improper means, since that would be unlawful and inadmissible (guide 117): the lawful boundary.
- **Proportionate and scoped:** the collection scoped to what the matter requires and minimised, given the breadth and sensitivity of account data (guide 20): the proportionate collection.

§ 0 6 · ADVANCED DATA PROTECTION

Advanced Data Protection and what changes

- **Optional end-to-end encryption:** Advanced Data Protection an optional setting that end-to-end encrypts much iCloud data, so that, for that data, only the user's trusted devices hold the keys (guide 133): the opt-in encryption.
- **Even Apple cannot provide it:** for ADP-protected categories, Apple unable to provide the data in readable form, so lawful process to Apple yields little for those categories (§5): the provider limit.
- **Establish whether it is on:** whether ADP is enabled established early, since it determines what lawful process to Apple can achieve, and what must instead come from a device or the account holder (guide 100): the status question.
- **Device and consent still work:** even with ADP, the data reachable via the user's own trusted device or with the account holder's consent and credentials, so ADP limits the provider route, not all routes (§5): the remaining routes.
- **State the effect honestly:** the effect of ADP on what can and cannot be obtained stated plainly, so expectations match reality (guide 100): the honest ADP account.

§ 0 7 · DEPLOYMENT

Deployment: the account as source and fallback

- **The account as primary source:** the iCloud account used as a first-class, often primary, source, aggregating the user's data more fully than any device (guide 130): the account as source.
- **Reaching evidence when the device is gone:** the account holding backups and synced data that reconstruct a lost, wiped or locked device's contents, so evidence survives the device (guide 130): the account as fallback.
- **Recovering older material:** old backups and offloaded data in the account recovering material the current device no longer holds (guide 147): the deeper history recovered.
- **Identifying undisclosed devices:** the account's device records revealing devices a party has not disclosed, opening further sources (guide 111): the hidden device found.
- **Lawful, proportionate, honest presentation:** the account data obtained lawfully, scoped proportionately, its ADP status 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 iCloud account is the hub of the Apple estate, and the devices are its spokes, so evidence flows both ways, the account aggregating the devices, and the devices holding what an ADP-protected account will not yield to the provider. The account holds photos, messages, backups, files, PIM, app and health data, and its own device and sign-in records. But the user's devices, iPhone, iPad, Mac, Watch (guides 145, 131, 157), hold the local, decrypted copies, which matter especially where ADP prevents Apple providing the cloud data; other cloud providers hold data synced from the same devices; and the counterparts hold their side of communications. The discipline is to treat the account as the real store and often the primary source, reached lawfully by consent, process or production, while recognising that where Advanced Data Protection is enabled the readable copy of protected data comes from a trusted device or the account holder, not from Apple. When a device is lost or wiped, the account's backups reconstruct it; when ADP blocks the provider route, the user's own device or consent supplies the data; and the account's device records reveal further sources to pursue. The account and the devices together, lawfully reached, give the fullest and most resilient picture.

EVIDENCE	ICLOUD ACCOUNT	USER'S DEVICES	VIA APPLE (NO ADP)	VIA APPLE (ADP ON)	CONSENT / DEVICE	COUNTERPART / OTHER CLOUD
Photos	Y: full library	Y: local copy	Y: producible	Limited (E2E)	Y: device/ consent	Shared copies
Messages	Y: if synced	Y: local	Some	Limited (E2E)	Y: device/ consent	Counterpart
Device backups	Y: incl. old devices	Source device	Y: producible	Limited (E2E)	Y: consent	n/a
Files / PIM	Y: synced	Y: local	Some	Limited (E2E)	Y: device/ consent	Other cloud
Account / device records	Y: sign-ins, devices	n/a	Y: producible	Y: metadata often available	Account holder	n/a

Fallback strategy in one line: treat the account as the real store, reached lawfully; where ADP blocks the provider route, obtain protected data from the user's trusted device or with consent, and use the account's device records to find further sources.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE WIPED PHONE AND THE INTACT ACCOUNT

A party wiped their iPhone before it could be examined, apparently destroying the evidence. The §4 account defeated the tactic: the §3 iCloud account behind the phone was intact, holding recent backups and synced photos, messages and files, and, reached §5 lawfully by production, it reconstructed much of what the wiped device had held (guide 147). The §4 account records also revealed a second device the party had not disclosed. The §6 ADP status was checked and the data obtained proportionately. Wiping the phone had not touched the real store. The lesson is §4's: the iCloud account often holds more, and survives, when a device does not, so wiping, losing or locking a phone frequently leaves an intact account behind it that reconstructs the device's contents and reveals further devices, making the account the route to evidence the device can no longer give, provided it is reached lawfully.

EXAMPLE 2 · ADVANCED DATA PROTECTION CHANGED THE ROUTE, NOT THE OUTCOME

Lawful process was served on Apple for an account's data, but much of it came back unavailable, because the account had §6 Advanced Data Protection enabled, so those categories were end-to-end encrypted and even Apple could not provide them. Rather than treat this as a dead end, the §6 remaining routes were used: the readable data was obtained from the account holder's own §8 trusted device and, in part, with §5 consent, since ADP limits the provider route, not all routes. The §6 effect of ADP was stated honestly. The evidence was obtained by a different lawful path. The lesson is §6's: Advanced Data Protection end-to-end encrypts much iCloud data so that even Apple cannot provide it, which changes the route to that data, from the provider to the user's own trusted device or consent, rather than necessarily defeating access, provided its status is established early and the honest effect stated.

EXAMPLE 3 · THE ACCOUNT THAT HELD THE OLDER HISTORY

A matter turned on data from some months earlier that the current phone no longer held, having offloaded and overwritten it. The §4 account held the history: an older §3 iCloud backup, and synced data retained in the account, preserved the earlier material the device had shed (guide 147), and, reached §5 lawfully and scoped §5 proportionately to the relevant period, it supplied what the device could not. The §7 deeper history was recovered from the account rather than the device. The account's longer memory answered the question. The lesson is §4's: because the account retains offloaded data and old backups, it often holds older material than the current device, so where a matter needs history the device has shed, the account is the source, reached lawfully and scoped proportionately to the period and data the matter genuinely requires.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating the device as the only source:** the cardinal error, examining the phone and forgetting the account that holds more (§2, §4).
- **Giving up when a device is gone:** assuming a wiped or lost device ends the enquiry, ignoring the intact account (Example 1, §4).
- **Improper access:** reaching the account by guessing credentials or unauthorised sign-in rather than lawfully (§5).
- **Not checking ADP:** serving process on Apple without establishing whether ADP makes the data unavailable (Example 2, §6).
- **Treating ADP as a dead end:** abandoning access when the device or consent route remains (§6).
- **Over-collecting:** taking the whole account without scoping to the matter (§5, guide 20).
- **Missing undisclosed devices:** not using the account's device records to find further sources (§4).
- **Ignoring older account history:** not recovering old backups and offloaded data the device no longer holds (Example 3, §4).

Technical limitations

- **Access is lawful only:** the account is reached only by consent, process or production, never improperly (§5).
- **ADP limits the provider route:** end-to-end encrypted data cannot be provided by Apple (§6).
- **Sync depends on settings:** what is in iCloud depends on what the user chose to sync (§3).
- **Breadth demands proportionality:** the account is broad and sensitive, so collection must be scoped (§5).
- **iCloud evolves:** what syncs and how it is protected changes over time (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the iCloud account likely to hold the relevant data, especially if a device is lost, wiped or locked?
- Is the account holder's consent available, or is lawful process to Apple or production the route, and is ADP enabled?
- What period and categories of data does the matter genuinely require, so collection is proportionate?

Ask your opponent

- Please preserve and disclose, proportionately, the relevant iCloud data (photos, messages, backups, files and app data) for the account at Schedule 1, and the account's device records.
- Please confirm whether Advanced Data Protection is enabled, and provide the data from a trusted device or by consent for any categories Apple cannot produce.
- Please confirm all devices signed in to the account.

Ask your eDiscovery / forensic provider

- What does the account hold, and does it have more or older data than the devices?
- How is the account reached lawfully, and how does ADP affect what can be obtained and by which route?
- What do the account's device records reveal, and how is the collection scoped proportionately?

SUGGESTED WORDING · INSTRUCTION FOR AN ICLOUD ACCOUNT ANALYSIS

> "We instruct you to examine the iCloud 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 and credentials, by lawful process served on Apple, or by production in disclosure) and never by improper means, and handling the data proportionately: (1) establish what the account holds, photos, messages, device backups (including of devices no longer in use), files, personal information, and app and health data, and whether it holds more or older data than the current devices; (2) establish whether Advanced Data Protection is enabled and, for any end-to-end-encrypted categories Apple cannot provide, obtain the readable data from the account holder's trusted device or with consent, stating the effect of ADP honestly; (3) recover older backups and offloaded data the current device no longer holds; (4) use the account's device and sign-in records to identify all associated devices, including any undisclosed; and (5) corroborate the account data with the devices, scope and minimise the collection, and present findings at honest confidence."

§ 12 · QUICK CONTROL

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

The iCloud account checklist

- ☐ Account treated as a first-class, often primary, source
- ☐ Access obtained lawfully (consent, process or production)
- ☐ ADP status established early
- ☐ End-to-end categories obtained via device or consent where ADP on
- ☐ Photos, messages, backups, files and app data recovered
- ☐ Older backups and offloaded data recovered
- ☐ Account device and sign-in records reviewed for other devices
- ☐ Account corroborated with the devices
- ☐ Collection scoped and minimised proportionately
- ☐ Effect of ADP and confidence stated honestly

Red flags

- The device treated as the only source; account forgotten: §4.
- Enquiry abandoned when a device is wiped or lost: Example 1.
- Account accessed improperly rather than lawfully: §5.
- ADP status not checked before process to Apple: Example 2.
- ADP treated as a total dead end when device/consent remain.
- The whole account collected without scoping.
- Undisclosed devices in the account records missed.

When to involve a digital forensic expert

Whenever an Apple user's data may live in the cloud, which is to say in most Apple matters, and always when a device is lost, wiped or locked, because the account is so often the real evidence store: the expert treats the iCloud account as a first-class, frequently primary, source, reached lawfully by consent, process or production, and establishes what it holds, photos, messages, device backups (including of devices no longer used), files and app data, often more and older than any device (Example 1, §4). Advanced Data Protection is checked early, and where it end-to-end encrypts data beyond Apple's reach, the readable copy is obtained from the account holder's trusted device or with consent, the route changed rather than the enquiry abandoned (Example 2, §6). Older history is recovered from old backups and offloaded data, the account's device records are mined for undisclosed devices (Example 3, §4), the collection is scoped proportionately, and findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, iCloud and account work recognises that for many users the evidence

lives in the account, not the device, and reaches it lawfully, proportionately and with a clear understanding of what Advanced Data Protection does and does not change.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Why look at iCloud rather than just the phone?

Because for many users the account, not the phone, is the real store (§2, §4). The device is a window onto an iCloud account that aggregates the data of all the user's devices and often holds more, and older, material than any one of them, offloaded data, backups of former devices, and full histories. It also survives when a device is lost, wiped or locked. So the account is frequently the richest single source, and sometimes the only route to evidence, which is why it is treated as a first-class source rather than an afterthought.

If a phone is wiped or lost, is the evidence gone?

Often not, because the account remains (§4, Example 1). Wiping, losing or locking a phone does not touch the iCloud account behind it, which typically holds recent backups and synced photos, messages and files that reconstruct much of the device's contents, and records of other devices too. Reached lawfully, the account frequently recovers what the device can no longer give. So the loss of a device is rarely the end of the enquiry; the account is the fallback that survives it, and is one of the first things to consider when a device is unavailable.

How is iCloud data obtained lawfully?

By consent, lawful process, or production (§5). The cleanest route is the account holder's informed consent and credentials; alternatively, lawful process (a court order or appropriate instrument) can be served on Apple to compel production of data Apple can provide; and a party can be required to disclose their own relevant iCloud data. Access is never obtained by guessing credentials or unauthorised sign-in, which would be unlawful and inadmissible. The route chosen depends on the matter, and the collection is scoped proportionately given the breadth and sensitivity of account data.

What is Advanced Data Protection and why does it matter?

It is Apple's optional end-to-end encryption for much iCloud data (§6, Example 2). When enabled, categories such as backups, photos and messages are encrypted so that only the user's trusted devices hold the keys, and even Apple cannot provide them in readable form. This matters because it changes what lawful process to Apple can achieve: for protected categories, the provider route yields little. But it limits that route, not all routes, the data remains reachable via the user's own trusted device or with their consent. So establishing whether ADP is on, early, determines how the data must be obtained.

Does the account show what devices someone has?

Yes, and that can be valuable (§4). An iCloud account keeps records of the devices associated with it and their sign-ins, so it can reveal devices a party has that were not disclosed, an old iPad, a second phone, opening further sources of evidence. These records also help establish who accessed the account and from where. So beyond its content, the account's own metadata is examined, both to identify all the relevant devices and to understand the pattern of access to the account itself.

Isn't collecting a whole iCloud account very intrusive?

It can be, which is why it is scoped and minimised (§5, guide 20). An iCloud account holds a vast and sensitive cross-section of a person's life, so collecting it wholesale is rarely proportionate. The collection is scoped to the categories and period the matter genuinely requires, minimised, and the data handled with heightened confidentiality and disclosed no more widely than necessary. This obtains the relevant evidence, of which the account often holds a great deal, while respecting the breadth and sensitivity of the material and the proportionality the UK GDPR and the rules require.

§ 14 · REFERENCE

Glossary

iCloud
Apple's cloud service behind its devices.

Apple Account
The account that owns a user's iCloud data.

iCloud backup
A cloud snapshot of a device's data.

Messages in iCloud
Message syncing to the account.

iCloud Photos
Photo syncing to the account.

Advanced Data Protection
Optional end-to-end encryption of iCloud data.

Lawful process
A legal instrument compelling production.

Consent route
Access by the account holder's permission.

Device records
The account's list of associated devices.

Offloaded data
Data moved off a device but kept in the account.

Sources and authoritative references

The iCloud and 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 (iCloud and account forensics, lawful cloud access, Advanced Data Protection awareness, 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 (lawful cloud collection as practised) and Phase 02 · Identification: 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
- Apple, iCloud data security overview and Advanced Data Protection (what is protected and how): support.apple.com, iCloud data security · Apple Platform Security guide: support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (lawful handling and honest reporting) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35 · UK GDPR (proportionate collection of account data): justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ico.org.uk

DISCLAIMER

This publication provides general information about iCloud and account forensics as at August 2026. What iCloud holds, and how it is protected, changes over time and depends on the user's sync settings, and access must be lawful: by the account holder's consent and credentials, by lawful process served on Apple, or by production in disclosure, never by improper means. Advanced Data Protection end-to-end encrypts much iCloud data so that even Apple cannot provide it, changing the route to that data. Account data is broad and sensitive and must be collected proportionately. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

iCloud and account work at the laboratory recognises that for many Apple users the evidence lives in the account, not the device, and reaches it lawfully, proportionately and with a clear understanding of Advanced Data Protection. The iCloud account is treated as a first-class, frequently primary, source, reached only lawfully, by the account holder's consent and credentials, by lawful process served on Apple, or by production in disclosure, and never by improper means (guide 117). Its contents are established, photos, messages, device backups including of devices no longer in use, files, personal information, and app and health data, and it is recognised that the account often holds more, and older, material than any current device, and survives a device that is lost, wiped or locked (Example 1, guide 147). Whether Advanced Data Protection is enabled is established early, and where it end-to-end encrypts data beyond Apple's reach, the readable copy is obtained from the account holder's trusted device or with consent, the route changed rather than the enquiry abandoned (Example 2). Older history is recovered from old backups and offloaded data, the account's device records are mined for undisclosed devices (Example 3), the collection is scoped and minimised given the breadth and sensitivity of account data, and findings are corroborated with the devices and reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding insight is that the device is often only a window, and the account behind it, reached lawfully, is where the real evidence store, and frequently the answer, is found.

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