COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Finding the Evidence

A Lawyer's Map of Modern Electronic Data Sources

Computers, phones, email, cloud systems, Teams, Slack, file servers, NAS, SaaS platforms, databases, CCTV, backups, CRM, ERP, social media, messaging applications, logs, IoT and third-party providers, where electronic evidence actually lives, how quickly it dies, how to reach it lawfully, and a comprehensive custodian and source questionnaire for answering the question every disclosure certificate quietly asks: have we identified all potentially relevant systems?

⏱ Estimated reading time: 32 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. Its eDiscovery arm, **e-discovery.uk**, begins every matter at exactly the point this guide addresses, identification of custodians, repositories and scope, logged as the first entry in the chain of custody, before forensic collection, processing, hosted review and production. Our examiners collect from every source category in this guide, from Microsoft 365 tenancies to locked handsets, DVR units and legacy servers, and produce CPR Part 35 and CrimPR Part 19 compliant expert reports where examination follows.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ISO 27001-ALIGNED SECURITY | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | MOBILE · CLOUD · ENDPOINT · SERVER COLLECTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

Every disclosure exercise, investigation and forensic instruction begins with the same unglamorous question: **where could the evidence be?** Twenty years ago the answer was a mail server and a shared drive. Today a mid-sized business generates potentially disclosable data across thirty or more distinct source categories, much of it outside the systems IT formally manages, some of it dying on a timer, and a meaningful share of it held by third parties the client has never thought of as "holding documents".

- **Identification is a duty, not housekeeping.** The preservation obligations in PD 57AD, the reasonable-search requirements of CPR 31.7, the DRD's data-source disclosure, and (in criminal work) the investigator's duty to pursue reasonable lines of enquiry all presuppose that the sources were competently found. You cannot preserve what you never identified, but you can be criticised for it.
- **Two maps, always.** The IT department's map (systems the organisation runs) and the custodians' map (where work actually happens: WhatsApp, personal drives, the spreadsheet on someone's desktop). Every identification failure in the reported cases lives in the gap between them.
- **Volatility sets the order of work.** CCTV overwrites in days; chat platforms purge on 30–90-day timers; leavers' accounts are deleted on schedule; logs rotate. §11's league table tells you what to preserve this week and what can wait for the CMC.
- **"All systems identified" is a process claim, not a knowledge claim.** Nobody can prove the negative. What you can prove is a defensible process: dual-track interviews, the cross-checks in §12 (finance records, SSO logs, MDM enrolment, mail-domain analysis), and a dated data map recording every inclusion, exclusion and reason.
- **The questionnaire does the heavy lifting.** §13 provides a comprehensive, reusable custodian and systems questionnaire, Part A for people, Part B for IT, Part C for the cross-checks, designed to be annexed to your identification file as the evidence of the process.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: why identification is a legal duty

Organisations no longer keep their records; their records keep themselves, everywhere. A single commercial decision now leaves traces in the decision-maker's mailbox, a Teams thread, a WhatsApp exchange, a SharePoint draft with version history, a CRM note, an ERP entry, a booking in the finance system, an entrance-badge log, and the mobile phones of everyone involved, plus copies in backup snapshots and, quite possibly, in systems run by an outsourced IT provider the client pays monthly and never thinks about. None of this was designed for litigation; all of it is potentially disclosable; and no single person in the organisation knows the whole picture.

The legal framework assumes you will deal with this competently:

- **PD 57AD** requires preservation of relevant documents once proceedings are contemplated, including notifying employees, former employees and relevant third parties, and the Disclosure Review Document requires the parties to describe their data sources, custodians and date ranges. A source you never found is a source the DRD misdescribes.
- **CPR 31.7 / PD 31B** frame the "reasonable search", expressly directing attention to the ease and expense of retrieval from particular sources, an assessment that cannot be made about sources nobody listed. PD 31B's Electronic Documents Questionnaire is, in substance, a source-identification form.
- **Criminal and regulatory work** raises the stakes: investigators must pursue all reasonable lines of enquiry (CPIA Code), and regulators' information notices assume the recipient can actually locate its data within the deadline.
- **The certificate concentrates the risk.** The disclosure statement or certificate asserts a search whose scope depends entirely on identification. The commonest route to a bad certificate is not dishonesty; it is a source map with holes.

> FOR THE PRACTITIONER
>
> Treat identification as an evidence-generating exercise in its own right. Its outputs, interview notes, the questionnaire returns, the data map with reasoned exclusions, are what you will produce when, eighteen months later, the opponent asks why the departed sales director's phone was never searched. "We asked, in writing, in week one, and here is the answer we received" is a complete answer. Memory is not.

§ 0 3 · READING THE MAP

How to read the map: custodians, systems, control and volatility

Four organising ideas make the source categories in §§4–10 usable rather than overwhelming:

- **Custodian view vs system view.** A custodian is a person whose data matters; a system is a place data lives. Every custodian maps to multiple systems (mailbox, laptop, phone, chat accounts, drives) and every system serves multiple custodians. Identification interrogates both axes: "what does Jane use?" and "who uses the ERP?", because each question surfaces sources the other misses.
- **Control, not possession.** Disclosure obligations attach to documents in a party's *control*, which reaches data held by agents, providers and (often) on employees' personal devices used for work, even though the party has never possessed it. The map therefore includes sources your client cannot touch without a request, a contract clause or a court order.
- **Volatility.** Each source carries a decay rate, from CCTV (days) to archived mail (years). The map notes it per category and §11 ranks it, because volatility, not importance, sets the order of preservation.
- **Access route.** For each source: who can lawfully extract it, with what (admin export, forensic tooling, provider request, court order), and what that route preserves or destroys. Identification without an access plan is a list, not a map.

§ 0 4 · THE MAP · ENDPOINTS

Computers, laptops, phones and tablets

Endpoints are where people actually work, and where the richest artefact evidence lives. They are also the most commonly destroyed source, through the most innocent process in IT: wiping and reissuing.

SOURCE	WHAT IT HOLDS	WHERE IT HIDES / WHAT LAWYERS MISS	VOLATILITY & ACCESS
Desktops & laptops	Local documents and downloads, mail caches (OST/PST), browser history, chat caches, recent-file and USB artefacts, deleted-but-recoverable data	Local folders that never sync; the previous user's profile on a reissued machine; personal laptops used for work (BYOD)	High on reissue/wipe cycles; forensic imaging preserves everything, admin copying does not
Smartphones	SMS/iMessage, WhatsApp and other app databases, call logs, photos with EXIF/GPS, voicemail, app data, location history	Work data on personal handsets; disappearing-message settings; the old phone in a drawer after upgrade	Very high (loss, replacement, purges); forensic extraction (logical/file-system) is the defensible route, screenshots are not
Tablets	Same families as phones plus shared-device use (shop floors, wards, sites)	Shared logins blur attribution; often outside MDM	Moderate; extract as phones
Removable media	USB sticks, external drives, SD cards, copies, exports, exfiltrated data	Never inventoried; matched to machines via USB registry artefacts	Physical loss; image on receipt, cross-reference to endpoint artefacts

IDENTIFICATION QUESTIONS THAT FIND ENDPOINTS

"What happens to a leaver's laptop, and when?" · "Do any staff use personal machines or phones for work, officially or not?" · "Where do replaced handsets go?" · "Is there an asset register, and does it match MDM enrolment?"

§ 0 5 · THE MAP · COMMUNICATIONS

Email, messaging applications, Teams, Slack and social media

SOURCE	WHAT IT HOLDS	WHERE IT HIDES / WHAT LAWYERS MISS	VOLATILITY & ACCESS
Corporate email (Exchange / M365, Google Workspace)	The core correspondence record: messages, attachments, calendars, headers	Recoverable-items folders; litigation-hold vs retention-policy gaps; shared and delegated mailboxes; distribution lists	Governed by retention policy, check and suspend it; export via Purview/Vault under protocol
Webmail & personal accounts (Gmail, Outlook.com, Proton)	Business conducted off-channel, often the candid version	Auto-forwarding rules from corporate mail; signatures in disclosed documents; custodian interviews	Outside client control: consent-based collection from the custodian, or third-party routes
Legacy archives (PSTs, Lotus Notes, journaling)	Pre-migration correspondence; the journal capture nobody remembers enabling	PSTs scattered on drives and old laptops; archive appliances still humming in a rack	Low volatility, high retrieval cost, scope early for the proportionality argument
Messaging apps (WhatsApp, Signal, Telegram, iMessage, SMS, WeChat)	Deals, instructions, admissions, the modern side-letter	Personal handsets; disappearing-message modes; linked-device desktop clients; cloud backups (iCloud/Google) that outlive the handset	Very high; forensic extraction from handset or backup, with the disappearing timer turned off in writing, day one
Teams / Slack / collaboration	Chats, channels, files, meeting recordings and transcripts, wikis	Private channels and DMs; org-wide retention timers (30–90 days is common); connected third-party apps	High until the timer is suspended; export scope varies by licence tier, verify what the tenancy can actually produce
Video platforms (Zoom, Meet, Webex)	Recordings, transcripts, in-meeting chat, attendance logs	Recordings saved to hosts' personal clouds; auto-transcripts nobody knows exist	Host-controlled retention; collect via admin console early
Social media (LinkedIn, X, Facebook, Instagram, TikTok)	Posts, DMs, connections, timestamps, location tags	Deleted posts surviving in platform archives; business conducted via LinkedIn DMs; employees' accounts vs corporate accounts	Platform-controlled; authenticated self-download archives > screenshots; third-party routes for opponents' accounts

§ 0 6 · THE MAP · STORAGE

File servers, NAS, cloud storage and backups

SOURCE	WHAT IT HOLDS	WHERE IT HIDES / WHAT LAWYERS MISS	VOLATILITY & ACCESS
File servers	Departmental shares, project trees, home drives, version history via shadow copies	Orphaned shares from reorganisations; access-permission records showing who could reach what	Low, but shadow copies rotate; targeted forensic copy of relevant trees
NAS devices	Small-office storage, camera footage, "the backup box" under someone's desk	Unmanaged, unencrypted, unlisted, classic shadow IT; often the only copy of something	Hardware failure and quiet reuse; image or targeted-copy on discovery
Cloud storage (OneDrive, Google Drive, Dropbox, iCloud, Box)	Documents with rich version history, sharing and access logs, deleted-item retention	Personal accounts synced to work machines; external sharing links; the "Personal" folder shared out two days before resignation	Deleted-item windows (30–180 days) and log-retention windows, collect activity logs, not just files
Backups (snapshots, appliance, tape, cloud, M365 retention)	Point-in-time copies, sometimes the only surviving version of deleted material	Rotation schedules silently overwriting the relevant snapshot; third-party backup providers; tape formats needing legacy hardware	Governed by rotation, a preservation decision in week one; restoration cost is a core proportionality argument (PD 31B addresses it directly)

FOR THE PRACTITIONER

Backups answer a different question from live systems: not "what exists?" but "what existed on date X?" That makes them the natural cross-check when deletion is suspected, and the reason a party that let its backup rotation run after the hold has an uncomfortable paragraph to write.

§ 0 7 · THE MAP · BUSINESS SYSTEMS

SaaS platforms, CRM, ERP, databases and finance systems

Structured systems hold the transactional truth of a business, and they do not produce "documents" in the ordinary sense. Identification here means finding the systems *and* establishing what reports, exports and audit trails each can generate.

SOURCE	WHAT IT HOLDS	WHERE IT HIDES / WHAT LAWYERS MISS	VOLATILITY & ACCESS
CRM (Salesforce, HubSpot, Dynamics)	Customer histories, contact notes, pipeline records, emails logged to records, user activity logs	Notes fields where salespeople write candidly; deleted-record recycle bins; per-user login and export logs (exfiltration evidence)	Recycle-bin windows; export via admin reports/API with field-level audit history where licensed
ERP (SAP, Oracle, NetSuite, Sage)	Orders, production, inventory, quality records, change logs	Transaction change-history tables proving who altered what, when; custom modules bolted on years ago	Low volatility; extract as agreed reports, never as raw dumps
Finance & accounting (Xero, QuickBooks, banking portals)	Ledgers, invoices, payment records, approval workflows, bank feeds	Audit trails recording edits to "historic" entries; attachment stores holding source invoices	Low; report-based export, with the audit trail expressly requested
Other SaaS (HR, ticketing, e-signature, project tools: Jira, Asana, Monday, DocuSign, Workday)	Approvals, task histories, signature certificates and audit trails, HR records	The estate nobody has listed, discovered via accounts payable and SSO logs (§12); e-signature audit certificates that prove (or demolish) execution dates	Provider-controlled retention; per-platform admin exports; contract terms govern access
Bespoke databases	Line-of-business data, often decades old	The retired developer who alone understands the schema; reports as the only sane extraction unit	Low volatility, high knowledge risk, identify the human dependency early

§ 0 8 · THE MAP · AMBIENT & PHYSICAL

CCTV, access control, telephony and the Internet of Things

SOURCE	WHAT IT HOLDS	WHERE IT HIDES / WHAT LAWYERS MISS	VOLATILITY & ACCESS
CCTV / DVR	Footage with (drifting) timestamps; export logs	DVR clocks minutes or hours wrong, synchronise before relying; overwrite cycles measured in days	**Extreme**, often 7–31 days; preserve by forensic export immediately, note the clock offset
Access control & alarms	Badge events, door logs, alarm set/unset, who was where, when	Managed by facilities, not IT; export formats vary wildly	Weeks to months; request early via building management
Telephony / VoIP	Call detail records, voicemails, call recordings (regulated sectors), softphone logs	Recordings retained under FCA rules the client forgot; mobile CDRs held by carriers, not the client	Carrier retention windows; provider requests or third-party orders
Vehicles	Telematics, sat-nav history, dashcams, infotainment phone pairings	Fleet-tracker portals (a SaaS source); the dashcam loop overwriting in hours	High for loops, moderate for portals; specialist extraction for on-vehicle units
IoT & smart devices (wearables, smart speakers/doorbells, industrial sensors, trackers)	Location, activity, audio events, sensor telemetry, in device, app and vendor cloud	The data is usually in the vendor's cloud, reached via the account, not the gadget	Vendor retention varies; preserve the account, then the device
Printers / scanners / MFDs	Job logs, scan-to-email history, sometimes stored images on internal drives	Lease returns wiping drives; logs proving a document was printed the night before resignation	Moderate; capture logs before lease churn

§ 0 9 · THE MAP · INFRASTRUCTURE & LOGS

Identity, network, MDM and audit trails

Logs rarely contain the story; they date, place and attribute it. They are also the fastest-rotating category after CCTV, and the one most likely to be discarded as "technical" until the attribution fight starts.

SOURCE	WHAT IT HOLDS	LITIGATION USE · VOLATILITY
Identity / SSO (Entra ID, Okta, Google)	Sign-in logs: who, when, from where, to which application; MFA events; the definitive list of connected SaaS apps	Attribution and timeline evidence; the §12 cross-check for unlisted systems · retention 30–90 days on default tiers, export early
M365 / Workspace audit logs	File access, sharing, downloads, mailbox actions, admin changes, eDiscovery activity	Exfiltration and tampering evidence · tier-dependent windows (90–180 days is common), a week-one export decision
Endpoint / security logs (Windows event logs, EDR)	Logons, USB events, process execution, remote access	The attribution backbone; malware/remote-access alternatives tested here · rotates by size, preserved best inside a forensic image
Network / proxy / DNS / VPN / Wi-Fi	What connected, to where, when; uploads to personal cloud; device presence on premises	Corroborates exfiltration and location · days-to-weeks rotation on default configs
MDM (Intune, Jamf)	Enrolled devices per user, compliance state, wipe commands	The device census against which the asset register is checked; a remote wipe after the hold is itself evidence · persistent while enrolled

§ 10 · THE MAP · THIRD PARTIES

Third-party providers, and the legal routes to their data

A substantial share of any client's evidence is held by someone else. Two questions per third party: is the data within the client's *control* (agents and contractors holding data on the client's behalf usually are, a preservation notice and a contractual request suffice), or genuinely a stranger's (carriers, platforms, counterparties, court-assisted routes may be needed)?

HOLDER	WHAT THEY HOLD	ROUTE TO THE DATA
Outsourced IT / MSPs	The client's own estate: backups, mail hosting, device management, ticket histories describing past incidents	Within control, written preservation notice day one; contract governs cooperation and exit
Accountants / auditors / payroll	Ledgers, working papers, correspondence, source documents	Usually within control for client records; professional-duty carve-outs for their own papers
Cloud & SaaS providers	The tenancy's data plus provider-side logs beyond the admin console	Admin export first; provider request under contract/DPA for the rest; preservation request to stop deletion timers
Telecoms carriers	Call detail records, subscriber information	Not within control, third-party disclosure application (CPR 31.17) or witness summons; regulatory/law-enforcement routes in criminal matters
Banks	Statements, payment records, KYC	Client's own records by mandate; others' via CPR 31.17 or *Bankers Trust* / *Norwich Pharmacal* relief in fraud claims
Counterparties & ex-employees	The other half of every conversation	Preservation letters immediately (cheap, and they found later spoliation arguments); disclosure through proceedings; springboard/delivery-up orders where justified
Platforms (social, marketplaces)	Account archives, deleted-content retention, access logs	User self-download with consent; *Norwich Pharmacal* for wrongdoer identification; platform legal-request processes

FOR THE PRACTITIONER

The third-party preservation letter is the highest-leverage document in this guide: one page, sent in week one, converting "they were never asked" into "they were on notice". Suggested wording is in §15.

§ 11 · DECAY RATES

The volatility league table: what dies first

Preservation order is set by decay, not importance. Typical default lifespans (verify per client, configurations vary):

RANK	SOURCE	TYPICAL SURVIVAL (DEFAULT CONFIGS)	WEEK-ONE ACTION
1	CCTV / dashcam loops	Hours to ~31 days	Forensic export today; record clock offset
2	Network / proxy / DNS / VPN logs	Days to weeks	Instruct IT to export and retain now
3	Chat platforms with retention timers (Teams, Slack)	30–90 days	Suspend the policy in-platform, day one
4	SSO / audit logs (M365, Google, Okta)	30–180 days by tier	Export the window; upgrade tier if needed
5	Leavers' accounts and devices	Per leaver process, often 30 days to deletion/reissue	Freeze the process; pull devices from the queue
6	Disappearing-message threads	Per timer, hours to 90 days	Timers off in writing; extract the handset
7	Cloud recycle bins / deleted-item retention	30–180 days	Litigation hold; export deleted-item stores
8	Backup rotations	Per schedule, the relevant snapshot may be next to be overwritten	Pause rotation for in-scope systems; catalogue snapshots
9	Handsets in circulation	Until lost, upgraded or reset	Extract key custodians' devices early
10	Live mailboxes, drives, servers under hold	Stable once held	Ordinary collection timetable
11	Archives, ERP history, completed backups	Years	Scope for proportionality; no urgency

Figure 1 · The decay league. Everything above rank 8 is a this-week decision regardless of where the CMC sits in the calendar.

§ 12 · THE COMPLETENESS QUESTION

"Have we identified all potentially relevant systems?" Proving a defensible process

The honest answer to the headline question is that no one can ever *know*; completeness is unprovable. What the court, the regulator and the certificate actually require is different and achievable: a **defensible identification process**, documented, with independent cross-checks that would have caught what interviews missed. Five cross-checks do most of the work:

CROSS-CHECK	WHAT IT CATCHES
1 · Dual-track interviews	Run IT/systems interviews (Part B) and custodian interviews (Part A) separately and compare. Divergence is signal: every system custodians mention that IT didn't list is shadow IT; every system IT lists that no custodian mentioned needs a use-check.
2 · Follow the money	Twelve months of accounts payable and corporate-card statements, filtered for software and subscriptions. Every SaaS platform the business actually uses is being paid for; finance finds the tools nobody thought to mention.
3 · Follow the logins	The SSO / identity provider's application list and sign-in logs are a census of connected systems per custodian, including the trial account someone connected two years ago that still holds project data.
4 · Follow the devices	Reconcile the asset register against MDM enrolment and mailbox-access device lists. Devices in one list but not another are exactly the unmanaged endpoints identification exists to find.
5 · Read the data you already hold	Sample the first-collected mailboxes for tell-tales: links to unlisted platforms, notifications from unknown SaaS, "moving this to WhatsApp", attachments whose paths reveal unlisted drives. The collected data audits the data map.

Close the loop in writing: the **data map** records every source found, its decision (collect / preserve-only / park / exclude) and the reason; the questionnaire returns and cross-check outputs are annexed; the map is versioned when late sources surface, because they will, and a documented late addition is routine while an undocumented one looks like concealment.

§ 1 3 · THE INSTRUMENT

The custodian and source questionnaire

Reproduce, adapt and annex. Part A goes to each custodian individually (in writing, with a signed return, or as a structured interview with notes); Part B to the IT function or MSP; Part C is completed by the legal team from records. The signed returns are the evidence of the identification process.

Part A · Custodian questionnaire (per person)

ROLE AND CONTEXT

- A1 · Your role, department, and involvement in the matters in dispute (dates included).
- A2 · Which colleagues, counterparties and third parties did you deal with on those matters?
- A3 · Have you changed role, location or employer during the relevant period?

DEVICES

- A4 · List every computer (work and personal) you have used for work in the relevant period, including replaced or returned machines.
- A5 · List every phone and tablet used for any work purpose, work-issued and personal, including old handsets you still have and any lost, replaced or reset in the period (with approximate dates).
- A6 · Do you use removable media (USB sticks, external drives)? Where are they now?
- A7 · Do you use any home or personal equipment for work (home PC, personal printer/scanner, home NAS)?

EMAIL AND ACCOUNTS

- A8 · List all email accounts used for any work purpose: corporate, personal/webmail, previous employers' accounts still accessible.
- A9 · Do you auto-forward, or have you forwarded, work email to any personal account?
- A10 · Do you keep local mail archives (PST files, exported folders)? Where?
- A11 · Does anyone else access your mailbox (delegates, assistants)? Do you access shared mailboxes?

MESSAGING AND COLLABORATION

- A12 · Which messaging apps do you use for anything work-related (WhatsApp, iMessage/SMS, Signal, Telegram, WeChat, LinkedIn messages, others)? For each: with whom, on which device(s), and whether desktop/web versions are linked.
- A13 · Are disappearing/auto-delete settings on in any relevant thread? Have you deleted any relevant chats, or left/cleared any relevant groups?
- A14 · Which collaboration platforms do you use (Teams, Slack, Zoom chat, project tools)? Any private channels or DMs relevant to the issues?
- A15 · Have any relevant meetings been recorded or transcribed? Where do those recordings live?

DOCUMENTS AND STORAGE

- A16 · Where do you actually save your work: which drives, sites, folders? Any locations only you use?

- A17 · Do you use personal cloud storage (personal OneDrive/Drive/Dropbox/iCloud) for anything work-related?
- A18 · Are there spreadsheets, databases or trackers you maintain that others rely on? Where are they?
- A19 · Do you keep paper that exists nowhere electronically (notebooks, diaries, signed originals)?

SYSTEMS

- A20 · List every business system you log into (CRM, ERP, finance, HR, ticketing, e-signature, sector systems), including any you signed up to yourself.
- A21 · Which of those systems contain material about the matters in dispute?

CONDUCT AND EVENTS

- A22 · Since the dispute arose (or since [date]), have you deleted, moved, exported, printed or "tidied" anything potentially relevant? Details, without judgment, candour now beats discovery later.
- A23 · Has any device been repaired, reset, upgraded or disposed of since [date]?
- A24 · Is there anywhere else, anywhere, that documents or messages about these matters might exist that we have not covered?

Signature block: I confirm the answers above are complete and accurate to the best of my knowledge, and I understand my preservation obligations. Name / date / signature.

Part B · IT and systems questionnaire (per organisation / MSP)

ESTATE AND INVENTORY

- B1 · Provide the systems inventory / asset register / data map, however maintained, with owners per system.
- B2 · Email platform(s), licence tier, and mailbox count; any journaling or archiving (current or historical)?
- B3 · Collaboration platforms in use (Teams, Slack, others), including tenancy count and any org-wide guest access.
- B4 · File storage: servers, NAS units, SharePoint/Drive structure; any storage not centrally managed?
- B5 · Business systems: CRM, ERP, finance, HR, and bespoke databases, with the person who understands each.
- B6 · SaaS estate: list all known subscriptions; provide the SSO/identity provider's connected-application list.
- B7 · Device fleet: asset register, MDM enrolment list, BYOD policy and reality.

RETENTION AND DELETION

- B8 · Current retention/deletion policies per platform (mail, chat, drives, recycle bins), and their actual configured values, not the policy document.
- B9 · What automatic deletion is scheduled to run in the next 90 days, on what?
- B10 · Backup regime: what is backed up, where, on what rotation; who operates it; when will the oldest relevant snapshot be overwritten?
- B11 · Leaver process: what happens to accounts, mailboxes and devices, on what timetable? Which relevant leavers are in that pipeline now?

LOGS AND SECURITY

- B12 · Log retention windows: SSO/sign-in, M365/Workspace audit, endpoint/EDR, VPN, proxy/DNS, Wi-Fi.

- B13 · Any security incidents, malware events or unusual-access alerts touching relevant custodians or systems in the period?
- B14 · Remote-access methods in use (VPN, RDP, remote-support tools) and their logging.

PHYSICAL AND AMBIENT

- B15 · CCTV: locations, retention/overwrite period, who can export, current clock accuracy.
- B16 · Access control / alarm systems and their log retention; managed by whom?
- B17 · Telephony: platform, call recording (what, why, retention), voicemail storage.
- B18 · Vehicles/plant: telematics or trackers, dashcams, and the portals they report to.
- B19 · Printers/MFDs: leased or owned; job-log availability; any lease returns pending?

THIRD PARTIES AND CHANGE

- B20 · All third parties holding or processing company data (MSP, hosting, backup, payroll, accountants, sector providers) with contracts and contacts.
- B21 · Migrations, decommissionings or system changes in the relevant period, and where the legacy data went.
- B22 · Anything scheduled (migrations, disposals, lease returns, office moves) that could alter or destroy data in the next 6 months?

Signature block for the responsible IT manager or MSP director, with an undertaking to notify the legal team before any change affecting listed systems.

Part C · Legal-team cross-checks (from records)

- C1 · Accounts-payable and corporate-card review (12 months) for software/subscription payments → reconcile against B6.
- C2 · SSO connected-application list and sign-in logs → reconcile against A20/B6; flag unlisted applications per custodian.
- C3 · Asset register vs MDM vs mailbox device-access lists → flag unmanaged devices per custodian.
- C4 · Sample review of first-collected mail/chat for references to unlisted platforms, drives or "let's take this offline" migrations.
- C5 · Contracts review: MSP, cloud and key-supplier agreements for data-access, retention and exit provisions.
- C6 · Record every discrepancy, its resolution, and the data-map version it changed.

§ 14 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Interviewing only IT.** The systems view is necessary and never sufficient; the candid material lives in the custodians' shadow map.
- **Asking custodians only about "documents".** People do not think of WhatsApp threads, voicemails or CRM notes as documents. The questionnaire asks about behaviour ("where do you actually save things?", "who do you message?"), not categories.
- **Treating the client's first answer as the answer.** "It's all in email" is a hypothesis to be cross-checked, not a scoping decision.
- **Ignoring decay while scoping.** Six careful weeks building the perfect data map, during which the CCTV overwrote, the Slack timer ran and two leavers' laptops were reissued.
- **Missing the third parties.** The MSP holding the backups, the accountant holding the ledgers, the carrier holding the CDRs, unasked, then unavailable.
- **No reasoned exclusions.** Parking the legacy archive is fine; parking it silently is a cross-examination gift. Every exclusion gets a sentence of reasoning in the map.
- **One-and-done identification.** Sources surface throughout the matter; a map without version history reads as a map that was never maintained.

Technical limitations

- **Licence tiers gate the evidence.** Audit-log depth, retention controls and export scope differ by subscription level; what the tenancy *can* produce is a fact to establish, not assume.
- **Provider-side data has windows.** Sign-in logs, sharing histories and deleted-item stores expire on provider schedules no hold notice can extend, only early export can.
- **Structured systems export answers, not archives.** CRM/ERP evidence arrives as reports; scoping means learning which reports exist and what the audit tables record.
- **BYOD access is negotiated, not commanded.** Personal devices engage the custodian's own rights; plan for consent, targeted extraction and transparency rather than seizure.
- **Some sources need the lab.** DVR exports, vehicle units, damaged or locked devices, legacy tape, identification can find them, but ordinary tooling cannot collect them.

§ 15 · INTERROGATORIES & DRAFTING AIDS

Questions for the opponent and the provider · Suggested instruction wording

Ask your opponent (DRD / EDQ / correspondence)

- Describe your identification methodology: who was interviewed, by whom, against what questionnaire; provide the source list with inclusions, exclusions and reasons.
- Confirm the position on messaging applications and personal devices for each custodian, expressly, not by silence.
- What retention and auto-deletion policies applied to each platform at the date the dispute arose, and when was each suspended?
- Which relevant custodians have left, and what happened to their accounts and devices, on what dates?
- What backup snapshots covering the relevant period existed when the hold was issued, and which survive?
- List third parties holding potentially relevant data and the preservation steps taken with each.

Ask an eDiscovery / forensic provider

- Which source categories in this guide can you collect in-house, mobile, cloud tenancy, DVR, vehicle, legacy media, and which would you subcontract?
- How quickly can you preserve the rank 1–7 volatility sources, and what does same-week mobilisation cost?
- What identification support do you offer: interview frameworks, SSO/finance cross-check analysis, data-map tooling?
- For provider-side sources (audit logs, deleted-item stores): what do you export by default, at which licence tiers?
- How are per-source collection decisions and exclusions documented for the DRD?

Suggested wording · Third-party preservation letter (core paragraphs)

> "We act for [client] in a dispute concerning [one line]. We understand you hold, or control, data relating to [client / the matters], including [categories, e.g. hosted mailboxes, backup archives, call recordings, ledger records]. Please treat this letter as formal notice to preserve all such data, and to suspend any deletion, overwriting, rotation or disposal process that would affect it, pending further communication. This includes automatic processes. Please confirm within [7] days: (1) the categories and date ranges of relevant data you hold; (2) the retention or deletion schedules that would otherwise apply; and (3) that preservation is in place. We will discuss scope, cost and any required authority on receipt. This request is made in contemplation of legal proceedings; failure to preserve may be drawn to the court's attention."

Suggested wording · Custodian identification instruction

> "Attached is a questionnaire about the devices, accounts, applications and systems you use for work. Please answer every question fully and candidly, including personal devices and accounts where they have been used for any work purpose, and return it signed by [date]. If you are unsure whether something counts, include it. Do not delete, move, export, 'tidy' or reorganise anything while the questionnaire is outstanding; preservation obligations are in force and are explained in the enclosed hold notice. Your answers will be relied on in describing the company's data sources to the court."

§ 16 · QUICK CONTROL

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

The identification checklist

- ☐ Hold issued before identification finishes; volatility ranks 1–7 preserved this week
- ☐ Part A questionnaires issued to every custodian; signed returns on file
- ☐ Part B completed by IT/MSP, with actual configured retention values, backup schedule and leaver pipeline
- ☐ Part C cross-checks run: finance, SSO, device reconciliation, collected-data sampling, contracts
- ☐ Data map drafted: every source → decision → reason; exclusions expressly reasoned; version control on
- ☐ Third parties listed; preservation letters sent; contract access routes confirmed
- ☐ Messaging apps and BYOD addressed per custodian, in writing
- ☐ Structured systems scoped by available reports and audit trails, with a named system owner each
- ☐ DRD Section 2 / EDQ drafted directly from the map
- ☐ Re-identification diarised (pleadings amendments, new custodians, disclosure review findings)

Red flags

- A custodian's questionnaire lists no messaging apps at all, in 2026, follow up in person.
- IT's system list and the SSO application list disagree by more than a handful of entries.
- Devices in the mailbox-access list that appear in no register and no questionnaire answer.
- A leaver "whose laptop was reissued last month", escalate: artefact recovery is time-critical.
- Retention policies that changed, or holds that were released, shortly after the dispute arose.
- An opponent's source list with no phones, no chat, no third parties and no exclusions, it is a first draft, treat it as one.
- Any answer to A22/A23 other than "no", route it down the forensic path, without drama and without delay.

When to involve a digital forensic expert

At identification stage, instruct a specialist when: a source needs laboratory access (locked/damaged devices, DVRs, vehicles, tape, legacy formats); a custodian's answers reveal deletion, resets or repairs since the dispute arose; BYOD or messaging-app extraction must be done once and defensibly; provider-side logs need expert scoping before their windows close; or the map itself will be contested and you want the identification methodology to carry an expert's imprimatur. Early involvement is cheap; the companion guides in this series (*eDisclosure or Digital Forensics?* and *The EDRM for UK Litigation Teams*) cover the escalation and lifecycle in full.

§ 17 · COMMON QUESTIONS

Frequently asked questions

Have we identified all potentially relevant systems?

You can never prove that you have; you can prove that you would have found what mattered. That means dual-track interviews (custodians and IT separately), the signed questionnaire in §13, and the five cross-checks in §12, finance records, SSO application lists, device reconciliation, sampling of collected data, and contract review, with every source, decision and reason recorded in a versioned data map. When a late source surfaces (one usually does), a documented process absorbs it as routine; an undocumented one turns it into an accusation.

Do we really have to deal with employees' personal phones and accounts?

Where they have been used for work on the matters in issue, yes, they are squarely in scope, and courts increasingly expect the DRD to address them expressly. The route is consent, targeted extraction (relevant apps, threads and dates, not the whole device) and transparency with the custodian, balancing the disclosure duty against their own data-protection rights. Silence on the topic is the one indefensible position.

How far do we go with backups?

Preserve first (pause the rotation for in-scope systems, cheap), restore later and selectively (expensive). PD 31B expressly treats accessibility and restoration cost as reasonable-search factors, so the defensible pattern is: catalogue what snapshots exist, preserve them, and negotiate restoration only where live sources cannot answer the question, typically where deletion is in issue.

Is CCTV really our problem in a commercial dispute?

Whenever physical presence, deliveries, meetings, access or timing could matter, yes, and it is the fastest-dying source on the map. The cost of a same-week forensic export is trivial; the cost of explaining a 14-day overwrite cycle to a judge is not. Check the DVR clock against real time when exporting and record the offset.

What about systems run by our IT provider, are they "ours" to disclose?

Data an MSP or provider holds on the client's behalf is generally within the client's control for disclosure purposes: the client must preserve and produce it, and the provider should receive a preservation notice on day one. Genuinely third-party data (carriers' records, platforms' logs, counterparties' files) is different, that is CPR 31.17, witness summons or *Norwich Pharmacal* territory, and the preservation letter still goes first.

Who should run identification, lawyers, the client, or a provider?

Lawyers own it (the outputs underwrite the certificate), the client's people supply it, and a provider accelerates it, particularly the technical cross-checks and volatile-source preservation. What must not happen is delegation to the client alone: self-identification has all the weaknesses of self-collection, one stage earlier.

§ 18 · REFERENCE

Glossary

BYOD
Bring your own device, personal hardware used for work, in scope where work data lives on it.

CDR
Call detail records, carrier-held metadata of calls and messages: numbers, times, durations, cells.

Control (CPR 31.8)
The disclosure test: physical possession, a right to possession, or a right to inspect or take copies, reaching agents' and providers' holdings.

Data map
The versioned record of sources, custodians, locations, volumes, volatility and scoping decisions with reasons.

DVR / NVR
Digital/network video recorders storing CCTV on short overwrite cycles, with independent (often wrong) clocks.

EDQ
PD 31B's Electronic Documents Questionnaire, the procedural source-identification form.

IoT
Internet of Things, connected devices (wearables, doorbells, sensors, vehicles) whose data usually lives in a vendor cloud.

MDM
Mobile device management, the enrolment system that doubles as a device census.

MSP
Managed service provider, outsourced IT holding the client's estate under contract.

NAS
Network-attached storage, office storage boxes, frequently unmanaged and unlisted.

Norwich Pharmacal order
Relief compelling a third party mixed up in wrongdoing to identify a wrongdoer or provide information.

Shadow IT
Systems and tools in real use without IT's knowledge or management, the custodian map's speciality.

Snapshot / rotation
A point-in-time backup copy, and the schedule on which older copies are overwritten.

SSO / IdP
Single sign-on / identity provider, the login layer whose application list censuses the SaaS estate.

Telematics
Vehicle-generated location and operation data, reported to fleet portals.

Sources and authoritative references

Source-handling practice in this guide draws on the EDRM phase notes and practice notes published by our e-discovery practice, referenced here as sources:

- e-discovery.uk, EDRM Phase 01 · Identification (custodians, repositories, scope, logged as the chain of custody's first entry): e-discovery.uk/edrm/identification
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection: e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, Knowledge Centre, including the practice notes on mobile evidence (Signal, WhatsApp and disappearing messages) and on when a logical extraction is enough: e-discovery.uk/knowledge
- e-discovery.uk, case notes on cross-border collection and personal-device protocols: e-discovery.uk/expertise
- Practice Direction 57AD (preservation duties; Disclosure Review Document): justice.gov.uk, PD 57AD
- CPR Part 31 (incl. 31.8 control; 31.17 third-party disclosure) and PD 31B with the EDQ: justice.gov.uk, Part 31 · PD 31B
- CPIA 1996 and Code of Practice (reasonable lines of enquiry): legislation.gov.uk/ukpga/1996/25
- Attorney General's Guidelines on Disclosure (rev. 2024, digital materials): gov.uk, AG's Guidelines

- ICO, UK GDPR guidance, including employment practices and monitoring: ico.org.uk
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21
- EDRM, Identification stage standards: edrm.net, stages standards

DISCLAIMER

This publication provides general information about electronic evidence identification in the United Kingdom as at August 2026. Retention periods, licence-tier capabilities and platform behaviours cited are typical defaults and vary by configuration; always verify against the client's actual estate. 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. Rules, guidance and legislation change; links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Identification is where our laboratory and our e-discovery practice (**e-discovery.uk**) are most often instructed together: examiners who can actually collect every source on this map, Microsoft 365 and Google tenancies, handsets (including locked and damaged devices), personal-device extractions under consent protocols, DVR and CCTV exports, vehicles, NAS units, legacy servers and tape, alongside an e-discovery team that runs the interviews, the finance and SSO cross-checks, and the data map that feeds DRD Section 2. Volatile sources are preserved same-week under laboratory chain of custody; everything else is scoped candidly, including the sources we advise are disproportionate to touch. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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