COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Control of Electronic Documents

What Lawyers Need to Investigate

Disclosure duties attach to documents within a party's control, and in the electronic estate that word does far more work than most case plans allow for. This guide explains the legal test and the practical investigation across subsidiaries and parent companies, employees and their personal devices, contractors, outsourced providers, cloud platforms, former staff and true third parties, with a decision tree, drafted wording and the questions that establish where control really lies.

⏱ Estimated reading time: 28 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**, runs defensible collections across exactly the boundaries this guide examines: group Microsoft 365 tenancies spanning parent and subsidiary, personal devices under solicitor-supervised consent protocols, data held by outsourced IT providers, and cloud accounts collected under documented lawful authority with chain of custody intact. Our examiners also produce CPR Part 35 and CrimPR Part 19 compliant expert reports and give evidence in UK courts and tribunals.

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

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE ANSWER: WHAT DOES "CONTROL" MEAN?

Under CPR 31.8, and to the same effect under PD 57AD, a document is or was in a party's control if the party has or had: (a) physical possession of it; (b) a right to possession of it; or (c) a right to inspect or take copies of it. Control therefore reaches far beyond the party's own servers: it captures documents the party has never seen, held by agents, providers, group companies and (through rights and arrangements) other people entirely. Disclosure and preservation duties both attach to the full width of that definition, which is why control is an investigation, not an assumption.

- **Control is about rights and arrangements, not geography.** Data in a provider's Irish data centre, a subsidiary's tenancy or an employee's pocket may all be in your client's control; data on your client's premises may not be (a contractor's own laptop, a director's personal phone absent the work-use facts).
- **The corporate veil holds, but arrangements pierce the practical question.** A parent does not control a subsidiary's documents merely by shareholding (*Lonrho v Shell*); it does control them where possession, an enforceable right, or a standing consent or arrangement to access exists in fact (*Pipia v BGEO Group*). In modern groups the shared IT tenancy often answers the question before company law does: whoever administers the tenancy has possession.
- **Employees' work material on personal devices is inside the exercise.** The courts have required parties to ask their employees and ex-employees to hand over work-related material on personal phones and email accounts (*Phones 4U v EE*), with privacy protected by protocol. Silence about BYOD is no longer a tenable disclosure position.
- **Agents and providers holding data for the client are the easy case.** Documents an MSP, accountant or cloud platform holds on the client's behalf are within control; the practical work is contracts, cooperation and preservation notices, not applications.
- **Where control genuinely ends, procedure begins.** Carriers, banks, counterparties and platforms are third-party territory: CPR 31.17, witness summonses, *Norwich Pharmacal* and *Bankers Trust* relief, and letters of request abroad.
- **Investigate early, record everything.** Control conclusions rest on facts (contracts, tenancy administration, BYOD practice, group arrangements) that must be gathered and documented in week one, because the DRD and the disclosure certificate will assert them.

§ 0 2 · FIRST PRINCIPLES

What "control" means in plain English

Disclosure has never been limited to documents a party physically holds. The rules ask a wider question: what documents can this party get at, as of right or through arrangements that exist in fact? Three limbs, in descending order of obviousness:

- **Physical possession.** For electronic documents, read this as systems possession: data on devices the client owns, in tenancies the client administers, on servers the client operates. Possession does not require awareness; the forgotten archive is possessed.
- **A right to possession.** Typically contractual: the MSP contract entitling the client to its hosted data; the employment contract making work product the employer's; the exit clause obliging a provider to hand everything back.
- **A right to inspect or take copies.** The widest limb: audit rights in supply contracts, information rights in shareholder agreements, access rights in agency and outsourcing arrangements, and (on the authorities) standing consents or understandings under which another person's documents are in practice available on request.

Three consequences follow that shape the whole exercise. First, **preservation tracks control**: the duty to preserve reaches documents held by third parties on the client's behalf, which is why preservation notices to providers and former employees go out on day one. Second, **control is time-sensitive**: the test includes documents that *were* in control, so a client that let a contract lapse or released data still has explaining, and listing, to do. Third, **control is asserted publicly**: DRD entries, disclosure statements and correspondence all state a control position, and an opponent is entitled to probe the facts behind it. The investigation in §12 exists to make those assertions safe.

§ 0 3 · THE LAW

The legal test and the leading authorities

AUTHORITY	WHAT IT DECIDES, IN PRACTICE
Lonrho Ltd v Shell Petroleum Co Ltd [1980] 1 WLR 627 (HL)	Shareholding alone is not control. A parent does not control its subsidiary's documents merely because it owns the subsidiary; there must be a presently enforceable right to obtain them (or possession, or an arrangement in fact). Separate corporate personality is respected.
North Shore Ventures Ltd v Anstead Holdings Inc [2012] EWCA Civ 11	Control extends to documents held by a third party where there is an arrangement or understanding, in fact, that the party can access them; a legally enforceable right is not essential if the documents are in practice available on request. Substance over form.
Pipia v BGEO Group Ltd [2020] EWHC 402 (Comm)	Applies that approach to modern groups: a holding company had control of subsidiaries' documents where standing consent and arrangements meant the data was available to it in practice, including data on group IT systems. The group-structure question is factual and evidence-led.
Phones 4U Ltd v EE Ltd [2021] EWCA Civ 116	Work-related material on employees' and ex-employees' personal phones and email accounts is within the reach of the disclosure process: the court can require a party to write to its custodians asking them to make such material available for search, under protocols protecting private content. The mechanism is the request, structured and supervised.

Distilled into working propositions:

- Control is a question of fact as much as law: contracts matter, and so do the arrangements actually operating (who can, and does, get the data on request).
- Group structures are analysed entity by entity, but shared IT collapses much of the analysis: tenancy administration is possession.
- For personal devices and accounts, the operative machinery is the structured request to the individual plus a privacy-protective protocol; refusals are then a documented fact the court can weigh.
- Assertions of no control are challengeable, and parties have been ordered to take steps (requests, enquiries) to convert practical availability into disclosure.

FOR THE PRACTITIONER

Note what the disclosure duty does and does not require. It requires the client to disclose and (where within control) produce; it does not make the client warrant that third parties will cooperate. Where control rests on a right or arrangement and the holder refuses, the client's obligation is to take the reasonable steps available (invoke the contract, make the request, escalate) and to record the refusal. The record of steps taken is the defence; silence is the sanction magnet.

§ 0 4 · THE CATEGORIES

Subsidiaries and parent companies

The classic control battleground. Work it in three layers:

- **Layer 1: the IT reality.** Before any company-law analysis, map the group's systems. A single Microsoft 365 or Google tenancy administered by the parent (or by a group services company) means the administrator has possession of every entity's mail and files in that tenancy; the same applies to group file servers, shared ERP instances and centralised backup. In most modern groups this layer answers most of the question.
- **Layer 2: rights.** Intra-group services agreements, data-sharing agreements, audit and information rights, board control provisions, and regulatory arrangements can each create a presently enforceable right to obtain a related entity's documents. Gather and read them; the DRD position should cite them.
- **Layer 3: arrangements in fact.** Even absent tenancy possession or contract, a standing consent or practice (the subsidiary routinely provides its documents to the parent on request; group legal accesses everything) can found control on the *North Shore* / *Pipia* approach. The evidence is emails, policies and witness confirmation of how the group actually operates, and it cuts both ways: your opponent's group may be similarly porous.

What to investigate: the group structure chart; tenancy and domain administration (who holds global admin, for which entities); intra-group agreements; where group legal, IT and HR functions sit; and the actual practice when one entity needs another's documents. **What to record:** a per-entity control conclusion with its basis, because "the Second Defendant's documents are not within the First Defendant's control" is an assertion the court can test against the tenancy admin list.

§ 0 5 · THE CATEGORIES

Employees, personal devices and personal accounts

Three zones, sharply different:

- **Company systems: unambiguous control.** Work mailboxes, chat accounts, drives and issued devices are the client's, whoever generated the content. No employee permission is needed to collect them (though employment-law fairness and UK GDPR transparency still apply to how it is done).
- **Work material on personal devices and accounts: inside the exercise, via the request.** Where custodians used WhatsApp, personal email or their own phones for work on the issues, *Phones 4U v EE* confirms the disclosure process can reach it: the employer writes to the custodian in agreed terms asking them to make work-related material available for search, typically through an independent process that screens out private content. The employer's contractual position helps (IT and BYOD policies asserting rights over work product; cooperation clauses) but the machinery is the structured request plus a protective protocol, and a refusal becomes a documented fact for the court.
- **Purely private material: outside it.** The exercise targets work-related content on the issues. Protocols exist precisely so that collection from a personal device does not become a trawl of someone's life: targeted extraction (relevant apps, threads, dates), independent handling, custodian review rights over plainly private items, and UK GDPR minimisation throughout.

What to investigate: BYOD and IT policies as written and as practised; which custodians actually used personal channels (the interview question set in our companion guide *Identifying the Right Custodians* surfaces this); employment-contract clauses on company documents and cooperation; and any prior practice of personal-device collection in the organisation. **What to record:** per custodian, the channels identified, the request made, the protocol offered, and the response.

§ 0 6 · THE CATEGORIES

Contractors and consultants

The analysis splits by where the work happened:

- **On client systems:** the contractor's activity in the client's tenancy, drives and business systems is simply the client's data. Include contractor accounts in the custodian and identity mapping; they are routinely forgotten because they sit outside HR's employee lists.
- **On the contractor's own systems:** control depends on the contract. Work-product and deliverables clauses, audit and records clauses, and return-of-materials provisions commonly give the client a right to possession or inspection of matter-related documents; general correspondence on the contractor's own servers may fall outside it. Read the actual agreement, including any agency's terms where staff came through an agency.
- **Hybrid reality:** the consultant who used a personal Gmail alongside the client-issued account, the development agency whose repository holds the only complete history. Treat each as a source, establish the contractual right, and send a preservation notice regardless: a holder on notice rarely deletes, whatever the later control argument.

What to investigate: the consultancy and agency agreements (IP, records, audit, return and survival clauses); which systems the contractor used on each side; and whether the engagement has ended, because exit obligations may already have crystallised a right to delivery-up.

§ 0 7 · THE CATEGORIES

Outsourced providers and managed services

MSPs, hosting companies, payroll bureaux, outsourced finance and records-storage providers hold the client's data as service providers: the paradigm case of control without possession. Practicalities:

- **Control is rarely in doubt; access mechanics are.** The contract (and, for personal data, the processor terms UK GDPR Article 28 requires) will contain access, assistance, return and deletion provisions. What varies wildly is speed, format and cost: an MSP's "we can restore that" may mean three weeks and a professional-services invoice. Establish the mechanics early and budget them.
- **The provider holds more than the service data.** Ticket histories describing past incidents and deletions, configuration records, backup catalogues and access logs are often provider-side documents about the client's estate. Ask for them expressly; they are frequently within control under assistance clauses, and always worth a preservation notice.
- **Provider changes are evidence events.** A migration between MSPs around the relevant period means two providers, an exit data set, and often a gap. Chase the exit deliverables and the old provider's residual holdings before contractual retention windows close.
- **Day-one action:** preservation notice to every provider on the third-party list, suspending deletion routines and backup rotations for the client's data, with a request to confirm holdings, schedules and the contractual basis of access.

§ 0 8 · THE CATEGORIES

Cloud platforms: your tenancy, their servers

The cloud question confuses because possession and infrastructure have come apart. Resolve it in two halves:

- **Tenancy data: the client's control, full stop.** Mail, files, chat and records inside the client's Microsoft 365, Google Workspace, Salesforce or other SaaS tenancy are within the client's control: the client administers the accounts and holds contractual rights to its data. "It's in the cloud" is never a reason a document cannot be disclosed, and courts treat cloud-hosted data exactly as they treat server-room data. Collection runs through admin tooling and APIs under documented protocols, with lawful authority recorded, and specialist collection preserves the metadata the export tools can drop.
- **Provider-side data: a narrower, contract-shaped right.** Logs and records the platform generates about the tenancy (sign-in histories beyond the admin console, infrastructure logs, deleted-data remnants after retention windows) belong to the provider's operation. Some are accessible under the contract or data-protection terms on request; some are not available at all; almost all expire on the provider's schedule. Establish per platform what exists, what the licence tier exposes, and what a formal request can add, and do it early, because provider-side windows are short.

Two recurring wrinkles. **Personal cloud accounts** (a custodian's own iCloud, Gmail or Dropbox holding work material) are analysed as personal accounts under §5: the request mechanism, not tenancy rights. **Consumer accounts used corporately** (the company Instagram registered to a founder's personal email; the WhatsApp Business number on an employee's SIM) need untangling: who is the account holder in the platform's terms, who has credentials in fact, and what does that mean for both control and preservation.

§ 0 9 · THE CATEGORIES

Former staff

Departure splits the analysis into what the company kept and what left with the person:

- **What the company kept is ordinary control:** archived mailboxes, retained exports, devices in storage, the leaver's footprint in shared and organisational systems. The urgent work is preservation (freeze the leaver pipeline) and inventory, covered in the companion custodian guide.
- **What left with the person is request territory.** Work material on a former employee's personal devices and accounts is reachable through the *Phones 4U* mechanism extended to ex-staff: a written request, in measured terms, offering an independent, privacy-protective extraction, supported by any surviving contractual obligations (return of company documents, confidentiality, cooperation clauses that survive termination). Responses, and refusals, are recorded; a refusal may ground further applications, and in exfiltration cases delivery-up and imaging orders against the individual directly.
- **Adverse leavers change the posture, not the analysis.** Where the former employee is the opposing party or aligned with them, the same material is pursued through the litigation itself: their own disclosure obligations, specific disclosure, and where justified preservation and imaging orders. The early preservation letter matters most precisely here: it converts later deletion from misfortune into conduct.

§ 10 · THE CATEGORIES

True third parties, and the routes to their documents

Where the investigation concludes there is genuinely no possession, right or arrangement, control ends and procedure takes over:

ROUTE	WHEN IT FITS
Voluntary request + preservation letter	Always first: cheap, fast, and it puts the holder on notice. Many third parties cooperate once scope, cost and confidentiality are addressed.
CPR 31.17 third-party disclosure	Documents likely to support or adversely affect a party's case, where disclosure is necessary: the workhorse order against carriers, banks, platforms and counterparties' service providers, with costs usually to the applicant.
Witness summons (CPR 34)	Production of specific documents at trial or a hearing; blunt but available where 31.17 does not fit.
***Norwich Pharmacal* relief**	The third party is mixed up in wrongdoing and holds information needed to identify a wrongdoer or plead a case: platforms, registrars, intermediaries.
***Bankers Trust* orders**	Tracing fraud through bank records: disclosure from banks about accounts through which claimant funds passed.
Letters of request / foreign procedures	The holder is abroad and beyond CPR reach: evidence requests through the foreign court, or the foreign jurisdiction's own third-party mechanisms (including, for US-held data, s.1782 applications).

The investigation feeds the route: an application under CPR 31.17 succeeds on specificity (which documents, why necessary), and the control analysis you performed, and recorded, is what demonstrates to the court that the documents cannot be obtained from the parties.

§ 11 · THE DECISION

The control decision tree

Run it per source or holder, and record the answer and its basis in the data map:

QUESTION 1

Does the client (or its administrators) have systems possession: the device, the server, the tenancy, the admin rights?

YES	NO
Within control, limb (a). Preserve and collect through ordinary channels; no third-party machinery needed.	Continue to Q2.

QUESTION 2

Does a contract or legal relationship give the client a right to possession or to inspect and copy (services agreement, employment terms, intra-group agreement, audit clause, processor terms)?

YES	NO
Within control, limb (b) or (c). Invoke the right in writing, send the preservation notice, diarise the response, and record the clause relied on in the DRD.	Continue to Q3.

QUESTION 3

Is there an arrangement or understanding in fact under which the documents are in practice available to the client on request (group practice, standing consent, habitual access)?

YES	NO
Arguably within control on the *North Shore / Pipia* approach. Gather the evidence of the practice, make the request, and take a reasoned DRD position either way.	Continue to Q4.

QUESTION 4

Is the holder an individual custodian or ex-custodian with work material on personal devices or accounts?

YES	NO
The *Phones 4U* mechanism: structured written request plus privacy-protective protocol; record responses and refusals; consider further orders if refused and the material is significant.	Outside control: choose the third-party route from §10, starting with the voluntary request and preservation letter.

Figure 1 · Four questions per holder. The output is not just a yes or no: it is the basis (possession, clause, arrangement, request) that the DRD, the certificate and any later argument will rest on.

§ 12 · THE INVESTIGATION

The investigation: what to gather and record

Control conclusions are only as good as the facts beneath them. The week-one gathering list:

GATHER	BECAUSE IT ESTABLISHES
Group structure chart and entity list	Which entities' documents need a per-entity control analysis, and who the litigating party actually is
Tenancy and domain administration records (global admins, per entity)	Systems possession across the group, the layer that usually decides the parent/subsidiary question
Intra-group services, data-sharing and audit agreements	Limb (b) and (c) rights between entities
MSP, hosting, SaaS and processor contracts (access, assistance, return, deletion, exit clauses)	Rights against providers, and the mechanics and cost of exercising them
Employment contracts, IT / BYOD / acceptable-use policies	The contractual backdrop to personal-device requests, and what the organisation told staff about work data
Contractor and agency agreements	Work-product, records and return rights over material on contractors' own systems
Evidence of arrangements in fact (how group requests actually work; who accesses what, routinely)	The *North Shore* / *Pipia* layer, in both directions
Custodian interview outputs on personal channels	Which individuals need the structured request, for which channels
Third-party holder list with relationship classification	Who gets a preservation notice, and which §10 route fits each true third party

Record the conclusions in a control schedule inside the data map: holder → documents → limb relied on (or "no control") → basis → action taken → response. That schedule drafts the DRD narrative almost by itself, and it is the exhibit that answers a control challenge two years later.

§ 1 3 · COMPLICATIONS

Cross-border complications

- **Control and local law can point in opposite directions.** An English court may hold a foreign subsidiary's data within the party's control while local data-protection, employment, secrecy or blocking statutes restrict its transfer. The answer is managed compliance, not paralysis: take local advice early, use targeted collection and in-country processing or review where transfer is the problem, apply UK GDPR transfer mechanisms where personal data moves, and put any genuine legal impediment before the English court with evidence rather than assertion.
- **Group tenancies blur borders.** Data "in" the German subsidiary may sit in a tenancy administered from London; where data resides, who administers it and which entity employs the custodian can be three different jurisdictions. Map all three before promising anything in the DRD.
- **Foreign providers answer to foreign process.** Where control is absent and the holder is abroad, plan the §10 routes with lead time: letters of request are slow, and US mechanisms (including s.1782) have their own tempo. Cross-border collection itself is routine for specialist providers, including remote acquisition under local supervision, but lawful authority must be documented per jurisdiction.
- **Sanctions and export controls** occasionally sit over data movement in disputes touching designated persons or controlled sectors; screen for them before data crosses a border, not after.

§ 14 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Equating control with the client's own systems.** The provider-held backups, the group tenancy and the contractor's repository silently omitted, then discovered by the opponent.
- **Equating group ownership with control, in either direction.** Asserting control over a subsidiary because it is "ours" (wrong absent possession, right or arrangement) or denying it despite administering the subsidiary's tenancy (worse).
- **Silence on BYOD.** A DRD that never mentions personal devices for custodians who plainly used them reads, correctly, as an unexamined exercise.
- **Requests drafted as demands.** The personal-device request works because it is measured and protocol-protected; a seizure-flavoured letter generates refusals and sympathy for the refuser.
- **Contracts unread.** Control positions asserted before anyone has read the MSP agreement's access clause or the consultancy's records clause.
- **Steps untaken and unrecorded.** Where control rests on a right or arrangement, failing to invoke it, or invoking it and not recording the response, converts a defensible position into an unevidenced one.
- **Letting provider windows expire during the analysis.** Weeks of careful control theorising while the platform's log retention and the old MSP's post-exit holding period quietly lapse.

Technical limitations

- **Rights do not conjure data.** A contractual right to data the provider has already deleted under its schedule yields nothing; that is why preservation notices precede control debates.
- **Admin access has edges.** Even global admins cannot reach everything (end-to-end encrypted content, some provider-side logs, another tenancy's data); establish per platform what tenancy control actually exposes.
- **Personal-device extraction depends on consent mechanics.** Targeted, protocol-based extraction is well developed, but device state, platform security and the custodian's cooperation set real limits; a specialist should scope feasibility before positions are taken in correspondence.
- **Arrangements in fact are provable both ways.** The email trail showing your client routinely pulled the subsidiary's records will surface in disclosure; take control positions your own documents support.

§ 15 · INTERROGATORIES

Questions to ask

Ask your client

- Who administers each tenancy, domain and shared system, and for which group entities?
- What intra-group agreements exist, and how do document requests between entities actually work in practice?
- Which providers hold company data (IT, hosting, backup, payroll, records storage), under what contracts, and who manages each relationship?
- What do the employment contracts and BYOD / IT policies say about work material on personal devices, and what is the real practice?
- Which contractors and agencies worked on the relevant matters, on whose systems, under what terms?
- For each relevant leaver: what did the company keep, what left with them, and what survives contractually?
- Has any provider, entity or individual ever refused or delayed a data request, and what happened?

Ask your opponent

- State your control position per group entity, with its basis: possession, right, or arrangement, and identify who administers each relevant tenancy.
- Confirm whether personal devices and accounts were used for relevant work by your custodians, and what requests under what protocol have been made.
- Identify providers holding relevant data on your behalf and the preservation steps taken with each, with dates.
- For any assertion that documents are outside your control: what steps have you taken to obtain them, and with what response?
- Have any contracts, arrangements or administrative rights relevant to control changed since the dispute arose?

Ask an eDiscovery / forensic provider

- How do you collect across a group tenancy while keeping per-entity provenance clean for the control schedule?
- What is your personal-device protocol: consent documentation, targeted extraction scope, private-content screening, custodian review rights?
- What provider-side data can you obtain per platform at our licence tiers, and what needs a formal request to the provider?
- How do you run cross-border collections: in-country options, remote acquisition, local supervision, transfer documentation?
- How is lawful authority recorded per source, so the chain of custody covers authority as well as integrity?

§ 16 · DRAFTING AIDS

Suggested wording for instructions

REQUEST TO A CUSTODIAN REGARDING PERSONAL DEVICES AND ACCOUNTS (CORE PARAGRAPHS)

"We are writing in connection with [the proceedings]. Because you used [WhatsApp / personal email / a personal device] for work matters relevant to the issues, we must ask you to make work-related material from those sources available for the disclosure exercise. The process is designed to protect your private information: an independent forensic laboratory will carry out a targeted extraction limited to [the identified applications, correspondents and date range]; plainly private material will not be reviewed by [the company]; you will have the opportunity to raise any items you consider private before anything is provided to the legal team; and your personal device will be returned [the same day where practicable]. Please confirm by [date] that you agree, and in the meantime do not delete, alter or dispose of any potentially relevant material, and disable any automatic-deletion settings on the relevant applications. If you have concerns, please raise them with [name] and we will seek to address them."

PRESERVATION AND ACCESS NOTICE TO A PROVIDER OR GROUP ENTITY (CORE PARAGRAPHS)

"We act for [client] in [proceedings]. Under [the services agreement dated … / the intra-group arrangements], you hold data belonging to or accessible by our client, including [categories]. Please: (1) preserve all such data and suspend any deletion, rotation or disposal process affecting it, including automatic processes and any post-termination deletion schedule; (2) confirm within [7] days the categories, systems, formats and date ranges of relevant data you hold, and the retention schedules that would otherwise apply; and (3) confirm the mechanism, timescale and any costs for providing our client with copies or access under [clause …]. Our client reserves all rights, and this letter may be shown to the court on questions of preservation and control."

DRD NARRATIVE: CONTROL STATEMENT (CORE PARAGRAPHS)

"The Claimant's control position is as follows. Documents on systems administered by the Claimant (including the group Microsoft 365 tenancy, which the Claimant administers for the entities listed) are within its control and have been preserved. Documents held by [provider] on the Claimant's behalf are within its control under [clause]; a preservation and access notice was sent on [date] and access confirmed on [date]. Work-related material on custodians' personal devices has been addressed by written requests under the protocol at Appendix [ ]; responses are recorded and the exercise will be updated as they complete. Documents of [entity] are not within the Claimant's control: the Claimant has no possession of its systems, no presently enforceable right to its documents, and no arrangement under which they are available on request; a voluntary request was nonetheless made on [date] and declined. The Claimant will keep this position under review."

§ 17 · QUICK CONTROL

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

The control checklist

- ☐ Group structure mapped; tenancy and domain administration established per entity
- ☐ Intra-group, provider, employment, BYOD and contractor agreements gathered and read for access, records and return clauses
- ☐ Every holder run through the decision tree; control schedule completed (holder → basis → action → response)
- ☐ Preservation notices sent day one to providers, group entities and relevant former staff
- ☐ Personal-channel usage established per custodian; structured requests issued under a privacy-protective protocol; responses logged
- ☐ Rights invoked in writing wherever control rests on a clause or arrangement; refusals documented
- ☐ Provider-side data and log windows established per platform; urgent exports done before they lapse
- ☐ Cross-border sources screened for local-law and transfer issues, with local advice where needed
- ☐ DRD control narrative drafted from the schedule, with reasoned no-control positions and steps taken
- ☐ Review diarised: control positions revisited on contract changes, staff departures and new sources

Red flags

- An opponent asserting no control over a subsidiary whose email visibly runs on the parent's domain.
- "Our provider handles all that" with no contract produced and no notice sent.
- A DRD silent on personal devices for custodians whose disclosed documents show WhatsApp exchanges.
- No-control assertions unaccompanied by any steps taken or requests made.
- Provider or tenancy administration changes shortly after the dispute arose.
- Your own client "confident" about group arrangements that no document supports.
- Refused custodian requests quietly dropped rather than recorded and escalated.

When to involve a digital forensic expert

Instruct a specialist when control questions become collection questions: personal-device extraction under consent protocols (done once, defensibly, with private material screened); group-tenancy collection with per-entity provenance; provider-side data that needs expert scoping before windows close; cross-border acquisition under local supervision; and any case where an imaging or delivery-up order is sought or resisted, where the examiner's methodology and independence carry the protocol. The companion guides in this series (*Finding the Evidence* and *Identifying the Right Custodians*) cover the wider source and custodian work this guide builds on.

§ 18 · COMMON QUESTIONS

Frequently asked questions

What does "control" of electronic documents mean?

Under CPR 31.8 and PD 57AD, a document is within a party's control if the party has or had physical (or systems) possession of it, a right to possession, or a right to inspect or take copies. In electronic practice that reaches the client's tenancies and devices, data held by providers and agents on the client's behalf, group companies' documents where possession, rights or standing arrangements exist, and, through the structured-request mechanism, work material on custodians' personal devices and accounts. It is established by investigation (contracts, tenancy administration, actual practice), asserted in the DRD, and testable by the court.

Do our parent's or subsidiary's documents count as ours?

Not automatically: shareholding alone is not control (*Lonrho*). But they do count where your client administers the relevant systems (shared tenancies decide many cases), holds contractual rights to the documents, or benefits from an arrangement in fact under which they are available on request (*North Shore*; *Pipia*). Analyse it entity by entity, and expect your opponent's group to be probed on the same basis.

Can we really be expected to deal with employees' personal WhatsApps?

Yes, where they were used for relevant work. The Court of Appeal in *Phones 4U v EE* endorsed exactly this machinery: the employer asks custodians, in agreed written terms, to make work-related material available for search under a protocol that protects private content. You are not seizing anyone's phone; you are making, and recording, a structured request, and a refusal becomes a fact the court can act on.

The data is in the cloud, so is it the provider's, not ours?

No. Data inside your client's tenancy is within your client's control: the client administers it and has contractual rights to it, and the courts treat it exactly like on-premises data. What sits outside easy reach is some provider-side material (certain logs, post-retention remnants), which is a narrower question of contract and request, and one to ask early because provider windows are short.

What if the foreign subsidiary refuses, or local law blocks transfer?

Take the steps the position allows and evidence everything: invoke the arrangements, make the request, take local advice on the restriction, propose managed alternatives (in-country processing and review, targeted extraction, transfer mechanisms), and put any genuine impediment before the English court with evidence. Courts distinguish sharply between parties who engaged with the problem and parties who deployed it.

Does control end when we no longer hold the document?

The duty catches documents that are *or were* in control: documents no longer held must still be identified in the disclosure exercise, with their fate stated. That is one more reason the control schedule records history (what was held, when, what happened to it) and not just the current position.

§ 19 · REFERENCE

Glossary

Arrangement in fact
A practice or standing consent under which another person's documents are in practice available on request; capable of founding control (*North Shore*; *Pipia*).

BYOD
Bring your own device: personal hardware used for work, addressed through structured requests and protocols rather than tenancy rights.

Control (CPR 31.8)
Possession, a right to possession, or a right to inspect or take copies, currently or in the past.

Control schedule
The per-holder record of control conclusions: basis, action taken, response; the backbone of the DRD control narrative.

Delivery-up
An order requiring a person to hand over documents or devices, typically in confidential-information and exfiltration cases.

Letter of request
A request from the English court to a foreign court for evidence from a person in that jurisdiction.

Norwich Pharmacal* / *Bankers Trust
Third-party relief for identifying wrongdoers and tracing funds through banks, respectively.

Preservation notice
The written notice to a holder (provider, entity, individual) to preserve data and suspend deletion processes.

Processor terms (UK GDPR Art 28)
Mandatory contract terms with data processors, including assistance, return and deletion provisions relevant to access mechanics.

Structured request
The *Phones 4U* mechanism: a written, protocol-protected request to a custodian to make work material on personal sources available for search.

Systems possession
Possession in the electronic estate: owning the device, operating the server, administering the tenancy.

Tenancy
An organisation's instance of a cloud platform (Microsoft 365, Google Workspace, a SaaS product), administered through its admin accounts.

Sources and authoritative references

Collection and protocol practice in this guide draws on materials published by our laboratory and e-discovery practice, referenced here as sources:

- e-discovery.uk, EDRM Phase 01 · Identification and Phase 03 · Collection (custodians, repositories and scope; forensic, hash-verified acquisition): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- e-discovery.uk, case notes including the solicitor-supervised personal-device collection protocol and cross-border regulatory disclosure across three jurisdictions: e-discovery.uk/expertise
- e-discovery.uk, UK Digital Forensics for US Litigation Teams (cross-border collections, UK GDPR compliance and remote acquisition): e-discovery.uk
- cflab.uk, Cloud Forensics (authorise, preserve, extract and report evidence from cloud accounts under chain of custody, with lawful authority established before acquisition): cflab.uk/cloud-forensics
- cflab.uk, Mobile Phone Forensics (the five-stage process and least-intrusive-method approach applied to consented personal-device extraction): cflab.uk/mobile-phone-forensics
- cflab.uk, Guides for defence lawyers and knowledge resources: cflab.uk/guides
- CPR 31.8 (control) and CPR 31.17 (third-party disclosure): justice.gov.uk, Part 31
- Practice Direction 57AD (control definition; preservation duties): justice.gov.uk, PD 57AD
- *Lonrho Ltd v Shell Petroleum Co Ltd* [1980] 1 WLR 627 (HL)

- *North Shore Ventures Ltd v Anstead Holdings Inc* [2012] EWCA Civ 11: bailii.org
- *Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm): bailii.org
- *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116: bailii.org
- ICO, UK GDPR guidance including international transfers and employment practices: 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

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Control questions become real at the moment of collection, and that is where our laboratory and our e-discovery practice (**e-discovery.uk**) operate together: group-tenancy collections with per-entity provenance kept clean for the control schedule; consented personal-device extractions under solicitor-supervised protocols that screen private material and document lawful authority; cloud-account acquisition with authority, hashes and chain of custody recorded from the first action (the discipline described on our cloud forensics pages at cflab.uk); provider-side data scoped and exported before platform windows close; and cross-border acquisition, remote or in-country, with transfer documentation handled. Where imaging or delivery-up orders are sought or resisted, our examiners act as the independent expert the protocol names, reporting under CPR Part 35 / CrimPR Part 19. 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