Finding The Evidence A Lawyers Map Of Modern Electronic Data Sources

Identifying all potentially relevant electronic data sources is a fundamental legal duty in UK litigation. This guide provides a lawyer's map, detailing various data types, their volatility, and practical methods for comprehensive identification, including questionnaires and cross-checks, to ensure a defensible e-discovery process.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
https://e-discovery.uk/library/finding-the-evidence-a-lawyers-map-of-modern-electronic-data-sources

DATA SOURCE IDENTIFICATION · A GUIDE FOR UK LAWYERS Finding the Evidence A Lawyer's Map of Modern Electronic Data Sources COMPUTER FORENSICS LAB · E-DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

§ 01 · ORIENTATION Executive summary

§ 02 · FIRST PRINCIPLES The problem in plain English: why identification is a legal duty FOR THE PRACTITIONER

§ 03 · READINGTHEMAP How to read the map: custodians, systems, control and volatility

§ 04 · THEMAP · END POINT S Computers, laptops, phones and tablets IDENTIFICATIONQUESTIONSTHATFINDENDPOINTS SOURCE WHAT IT HOLDS VOLATILIT Y & ACCESS WHERE IT HIDES / WHAT LAWYERS MISS

§ 05 · THEMAP · COMMUNICATIONS Email, messaging applications, Teams, Slack and social media

§ 06 · THEMAP · STORAGE File servers, NAS, cloud storage and backups

§ 07 · THEMAP · BUSINESS SYSTEM S SaaS platforms, CRM, ERP, databases and finance

systems

§ 08 · THEMAP · AMBIENT & PHYSICAL CCTV, access control, telephony and the Internet of Things

§ 09 · THEMAP · INFRASTRUCTURE & LOGS Identity, network, MDM and audit trails SOURCE WHAT IT HOLD S LITIGATION USE · VOLATILIT Y

§ 10 · THEMAP · THIRDPARTIES Third-party providers, and the legal routes to their data HOLDER WHAT THEY HOLD ROUTE TO THE DATA

§ 11 · DECAYRATES The volatility league table: what dies first RANK SOURCE WEEK-ON E ACTION T YPICAL SURVIVAL (DEFAULT CONFIGS) 1 CCTV / dashcam loops Hours to ~31 days Forensic export today; record clock 3 Chat platforms with retention timers 30-90 days Suspend the policy in-platform, day 4 SSO / audit logs (M365, Google, Okta) 30-180 days by tier Export the window; upgrade tier if 5 Leavers' accounts and devices Per leaver process, often 30 Freeze the process; pull devices from 6 Disappearing-message threads Per timer, hours to 90 days Timers off in writing; extract the 7 Cloud recycle bins / deleted-item 30-180 days Litigation hold; export deleted-item 8 Backup rotations Per schedule, the relevant Pause rotation for in-scope systems; 9 Handsets in circulation Until lost, upgraded or reset Extract key custodians' devices early 10 Live mailboxes, drives, servers under Stable once held Ordinary collection timetable 11 Archives, ERP history, completed Years Scope for proportionality; no urgency

§ 12 · THECOMPLETENESSQUESTION "Have we identified all potentially relevant systems?" Proving a defensible process CROSS-CHECK WHAT IT CATCHES 1 · Dual-track interviews Run IT/systems interviews (Part B) and custodian interviews (Part A) separately and 2 · Follow the money Twelve months of accounts payable and corporate-card statements, filtered for software 4 · Follow the devices Reconcile the asset register against MDM enrolment and mailbox-access device lists. 5 · Read the data you already Sample the first-collected mailboxes for tell-tales: links to unlisted platforms, notifications

§ 13 · THEINSTRUMENT The custodian and source questionnaire Part A · Custodian questionnaire (per person) ROLEANDCONTE XT DEVICES EMAIL AND AC COUNTS MESS AG INGANDCOLLABOR AT ION DOCUMENTS AND STORAGE SYSTEMS CONDUCTANDEVENTS Part B · IT and systems questionnaire (per or g an is at i on / MSP) ES TAT EANDINVENTORY RETENTIONANDDELETION LOGSANDSECURITY PHYSICALANDAMBIENT THIRD PA RTIESANDCHANGE Part C · Legal-team cross-checks (from records)

§ 14 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 15 · INTERROGATORIES & DRAFTING AIDS Questions for the opponent and the provider · Suggested instruction wording Ask your opponent (DRD / EDQ / correspondence) Ask an e Discovery / forensic provider Suggested wording · Third-party preservation letter (core paragraphs) Suggested wording · Custodian identification instruction

§ 16 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The

identification checklist Red flags When to involve a digital forensic expert

§ 17 · COMMON QUESTIONS Frequently asked questions Have we identified all potentially relevant systems? Do we really have to deal with employees' personal phones and accounts? How far do we go with backups? Is CCTV really our problem in a commercial dispute? What about systems run by our IT provider, are they "ours" to disclose? Who should run identification, lawyers, the client, or a provider?

§ 18 · REFERENCE Glossary BYOD CDR DVR / NVR EDQ MDM MSP Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 in defensible 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 export in g 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915