Guide 5 Identifying The Right Custodians In Electronic Disclosure

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/guide-5-identifying-the-right-custodians-in-electronic-disclosure

CFLELECTRONICEVIDENCESERIES · GUIDE5Identifying the RightCustodians in ElectronicDisclosureCustodians, non-custodial sources, shared mailboxes, service accounts andformer employees: a practical guide to building, prioritising and defending thecustodian list - with a full custodian interview question bank.COMPUTER FORENSICS LABContents1 Executive summary2 Custodians in plain English3 Why custodian selection matters legally4 Key terminology5 Custodial and non-custodial sources6 Building the custodian list: a practical workflow7 Tiering, prioritisation and proportionate custodian counts8 Special categories of custodian9 Decision tree: should this person or source be a custodian?10 The custodian interview and question bank11 Worked examples: Aldgate Components v Harlow Precision12 Custodians in the DRD and negotiating with opponents13 Preservation and legal hold considerations14 Collection, metadata and attribution considerations15 Privilege and confidential it y16 UK GDPR and data minimisation17 Common mistakes18 Technical limitations19 Questions to ask the opponent and your provider20 Model wording21 Custodian identification checklist22 Red flags23 When to involve a digital forensic expert24 Scotland, Northern Ireland, arbitration, tribunals and criminal proceedings25 Glossary26 References and further reading27 How a specialist laboratory can assist28 DisclaimerKEY MESSAGESEXECUTIVE SUMMARYTHE CORE PROBLEMCUSTODIANS IN PLAIN ENGLISH3.1 PD57AD and the Disclosure Review Document3.2 CPR Part 31 cases3.3 What goes wrongWHY IT MATTERS LEGALLYPRACTICE POINTCCTV.KEY TERMINOLOGY5.1 Shared and functional mailboxes5.2 Departmental repositories5.3 Service accounts, bots and integrations5.4 Systems of record and structured data5.5 Archives, journals and backupsRULE OF THUMBCUSTODIAL AND NON-CUSTODIAL SOURCESDELIVERABLEBUILDING THE CUSTODIAN LIST7.1 A three-tier model7.2 Techniques that keep counts honestTIERING AND PROPORTIONALITY8.1 Former employees8.2 Personal assistants and delegates8.3 Senior executives and board members8.4 Contractors, agency staff and out sourced functions8.5 Personal devices and personal accounts (BYOD)SPECIAL CATEGORIES8.6 Group companies and overseas custodians40 (multi-jurisdictional collection) address this in detail.LEAVER? PERSONAL SOURCES? OTHER ENTITY / ABROAD?DECISION TREE10.1 How to run it10.2 Question bankTHE CUSTODIAN INTERVIEWCROSS-REFERENCEEXAMPLE 1 · THE SIGNATORY IS NOT THE NEGOTIATOREXAMPLE 2 · THE LEAVER ON A 60-DAY TIMEREXAMPLE 3 · SAMPLING THE MARGINAL CUSTODIANSWORKED EXAMPLE S12.1 Completing Section 2 of the DRD12.2 Negotiating custodian listsCUSTODIANS IN THE DRDPRESERVATION AND LEGAL HOLDCOLLECTION AND ATTRIBUTIONUK GDPR AND DATA MINIMISATIONCOMMON MISTAKESTECHNICAL LIMITATIONSQUESTIONS TO ASKWording A · Instruction to the client to convene custodian identificationWording B · Custodian paragraphs for a hold noticeWording C · Proposing custodians to the opponentWording D · Instructing the provider on custodian collectionsMODEL WORDINGTREAT ANY OF THESE AS A STOP-AND-ESCALATE

SIGNALCHECKLIST24 Scotland, Northern Ireland, arbitration, tribunals and criminalproceedingsWHEN TO INVOLVE AN EXPERTBYODDRDJMLMDMPSTGLOSSARYREFERENCESHOW A SPECIALIST LABORATORY CAN ASSISTINSTRUCTTHELABNEWENQUIRIES+44 (0)20 7164EMAILinfo@cflab.ukE-DISCOVERYe-discovery.uk

Questions and answers

Which individuals involved in the events in issue have you excluded, and why?

Which relevant custodians have left your or g an is at i on? For each: what has happened to their mailbox, files, chat data and devices, and on what dates? What steps have you taken to preserve custodian data - including suspension of deletion policies, JML freezes and device quarantine - and when? Did relevant individuals use personal devices or accounts (including messaging apps) for the matters in issue, and what steps have you taken in respect of that material? Which shared mailboxes, department a l repositories and systems of record will you search in addition to individual custodians? What de-duplication approach will you apply, and will your productions preserve full custodian information for each document? 1. 2. 3. 4. 5. 6. 7. TECHNICAL LIMITATIONS CFL Electronic Evidence Series · Guide 5 Page 23 Ask the forensic / e Disclosure provider For each custodian and source on our register, what collection method do you recommend, and what will it capture and miss?

How will you verify and document that each collection is complete and attributable (hashes, logs, chain of custody)?

Can you run early data assessment on Tier 1 to map communication patterns and test marginal custodians before we commit to full processing?

How does your platform record custodian metadata, and how is cross-custodian de-duplication handled - is an all custodians field maintained and producible?

For leavers: what are the realistic recovery options per source (converted mailboxes, archives, backups, PST exports), and in what order should we try them? For personal devices and accounts: what independent-examiner protocol do you offer, what filter in g is applied, and who sees what at each stage? Where will custodian data be hosted, who can access it, and what happens to it at the end of the matter (retention, return, certified deletion)? 1. 2. 3. 4. 5. 6. 7. QUESTIONS TO ASK CFL Electronic Evidence Series · Guide 5 Page 24 20 Model wording Adapt to the matter; none of this is a substitute for advice on the facts. Wording A · Instruction to the client to convene custodian identification "To enable us to comply with the disclosure obligations that now apply, please arrange for us to speak with: (i) the person best placed to describe your IT systems, retention policies and leaver processes; (ii) the heads of the departments involved in [the events]; and (iii) the individuals listed in the attached schedule. Each conversation will take 30-60 minutes and will cover their role, communications, devices, accounts and document locations. Please do not ask anyone to gather, tidy or delete material in advance; the purpose is to find where documents are, and nothing should change until we have spoken. Please also tell us immediately of any listed individual who has left or is about to leave, so that their accounts and devices can be preserved today." Wording B · Custodian paragraphs for a hold notice "You have been identified as a person who may hold documents relevant to [the dispute]. 'Documents' includes emails, chat and text messages (including Whats App and similar apps, on work or personal devices), documents and their drafts, spreadsheets, notes, calendars, voicemails and recordings, wherever stored - including personal devices and personal accounts if used for work. From now: (1) do not delete, alter or dispose of any such material; (2) switch off any disappearing-message settings in chats relating to [the matter]; (3) do not reset, replace, repair or return any device that may contain such material without

first contacting [name]; (4) confirm by reply that you have read and will comply with this notice. If in doubt, keep it and ask." Wording C · Proposing custodians to the opponent "Our client proposes to search the documents of the following custodians, whose roles and date ranges are set out in the enclosed schedule: [list]. These individuals were identified from the statements of case, interviews conducted with [n] members of staff, and analysis of communication patterns in an initial dataset. Our client will additionally search the following non-custodial sources: [shared mailboxes; repositories; systems]. We have preserved, but do not presently propose to search, the documents of [names/roles], for the reasons given in the schedule; our client will keep that position under review and invites your comments. Please provide the equivalent information for your client, including in respect of former employees and any relevant personal devices or accounts." Wording D · Instructing the provider on custodian collections "Please collect, for each custodian listed in Schedule 1, the sources identified against their name, apply in g the date ranges stated. Collections are to be forensic all y sound and documented: for each, record custodian, source, method, tool and version, o per at or, date/time, scope applied and verification hashes, and maintain chain-of-custody records. Custodian attribution must be preserved through processing; apply global de-duplication only if all custodians holding each document remain recorded and reportable. Personal devices and accounts listed in Schedule 2 are to be handled under the independent-examiner protocol at Schedule 3 [scope; filter in g; who sees what; return/deletion of out-of-scope material]. Host all data in [the UK/EEA]; at the conclusion of the matter, retain for [period] and then delete with certification. Report anything suggesting data loss, wiping or tampering immediately and before further processing." MODEL WORDING CFL Electronic Evidence Series · Guide 5 Page 25 21 Custodian identification checklist 22 Red flags TREAT ANY OF THESE AS A STOP-AND-ESCALATE SIGNAL A key actor resigned shortly before or after the dispute arose - and nobody has checked what happened to their account and devices. IT cannot say what the leaver process did to a named individual's mailbox, or the answer changes between askings. A custodian's interview answers conflict with system records (accounts or devices they "never used" show recent activity - or the reverse). Unexplained gaps: an obvious custodian has almost no documents for a critical period, or a thread's replies exist without the originals. A custodian "tidied up", ran a cleaner tool, or factory-reset a phone after the hold notice. Work was conducted in personal channels and the custodian is reluctant to discuss preservation of them. The opponent's custodian list omits the individuals your documents show at the centre of events, or refuses date ranges and reasons. Devices of departed custodians were reissued or recycled after litigation was in contemplation. Delegates or shared accounts sent key documents "as" a principal who denies knowledge. Several of these fall within later guides on deleted evidence and destruction investigations (Guides 27-30). The immediate steps are always the same: preserve what remains, document the state of things as found, and take specialist advice before anyone touches the source again. Issues extracted from statements of case and translated into events, actors, periods and systems Period-specific org charts, project lists and HR joiners/movers/leavers report obtained IT / organisational-knowledge interviews completed (systems, retention, JML, archives) Candidate custodian list assembled; custodian and source register opened Hold notices with privacy notice sent to all candidates; acknowledgements logged and chased Per-custodian IT preservation actions completed (mailbox/OneDrive holds, retention suspensions, device quarantine) Leavers: account status confirmed in writing;

deletion timers frozen; archive/backup coverage checked Custodian interviews completed on the standard template; snowball names fed back into the register Personal-source use identified; preservation requests sent; independent-examiner protocol agreed where needed Shared mailboxes, department a l repositories, service accounts and systems of record listed as non-custodial sources Tiers assigned; inclusion/exclusion reasons recorded; sampling/EDA evidence filed for marginal decisions DRD Section 2 populated from the register (custodians, ranges, sources, unavailable data explained) Opponent's custodian list obtained with reasoning; their leavers and personal sources questioned De-duplication approach confirmed to preserve full custodian history Register reviewed at each milestone; holds re-verified before DRD certification and production CHECKLIST CFL Electronic Evidence Series · Guide 5 Page 26 23 When to involve a digital forensic expert Routine custodian collections from live corporate systems are e Disclosure work. Involve a digital forensic specialist when the custodian exercise itself raises questions only forensic methods can answer: Leaver reconstruction. Recovering or reconstructing a departed custodian's data from converted mailboxes, archives, backups, reissued devices or unallocated space - and evidencing what was lost, when and by what process. Personal devices and accounts. Acting as the independent examiner in a Phones 4U-style protocol: defensible extraction, filter in g personal material, and reporting within an agreed scope. Attribution disputes. Establishing who used an account or device at the material time from authentication logs, artefacts and device evidence - including delegate-send and shared-login situations. Suspected spoliation. Any red flag in