Known Adverse Documents In The Digital Age

This guide addresses the identification of known adverse documents in the digital age, focusing on methodology, employee knowledge, and unusual repositories. It outlines an identification programme, discusses handling adverse finds, and highlights common mistakes.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
https://e-discovery.uk/library/known-adverse-documents-in-the-digital-age

KNOWNADVERSEDOCUMENTS · A GUIDE FOR UK LAWYERS Known Adverse Documents in the Digital Age Methodology, People and the Places Nobody Searches COMPUTER FORENSICS LAB DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: THEDUTY, ANDTHETHREEPILLARSOFPERFORMINGIT

§ 02 · FIRST PRINCIPLES The problem in plain English: a human duty in a machine estate

§ 03 · THELAW The legal anatomy of the duty

§ 04 · THESHIFT Why the digital age changes everything DIGITAL REALIT Y CONSEQUENCE FOR THE DUT Y

§ 05 · PILLAR1 Search methodology matters

§ 06 · PILLAR2 Employee knowledge matters

§ 07 · PILLAR3 Unusual repositories matter

§ 08 · METHOD The identification programme, step by step STEP ACTION AND OUTPUT 2 · Census the knowledge List the people whose awareness counts (events and litigation-conduct), including leavers; 3 · Ask the adverse question Census interviews with the direct question, safely framed; privileged notes with factual 4 · Design the search Both-vocabulary terms, adverse coding in the protocol, TAR trained on relevance, 7 · Disclose on the timetable With Extended Disclosure or within the fallback timetable; late-arising knowledge disclosed 8 · Refresh on triggers Amendments, witness statements, new custodians, significant finds: steps 2 to 5 re-run for

§ 09 · WHENITHAPPENS Handling an adverse find

§ 10 · IN THE WILD Worked examples EXAMPLE1 · THEINCIDENTLOGNOBODYCONNECTED EXAMPLE2 · THELEAVERWHOANSWEREDHONESTLY EXAMPLE3 · TWOREVIEWROOMS, ON E DOCUMENT

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

§ 12 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · THECENSUSINTERVIEWQUESTION (FOR THE NOT E)

§ 13 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The known-adverse checklist Red flags When to involve a digital forensic expert

§ 14 · COMMON QUESTIONS Frequently asked questions What makes a document "adverse"? Whose knowledge counts as the company "knowing"? Do we have to go looking for adverse documents? What if the adverse document is privileged? We have just found something bad, late in the case. Now what? How does this play in criminal and regulatory matters?

§ 15 · REFERENCE Glossary 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

What makes a document "adverse"?

It contradicts or materially damages your contended version of events on the issues in dispute, or supports your opponent's. The anchors are the pleaded issues and material it y: a document that is merely unflattering, or damaging on something not in issue, is not within the duty (though it may still fall within an ordered search). Marginal calls are legal judgments, made by counsel and recorded with reasons in the escalation log.

Whose knowledge counts as the company "knowing"?

People with accountability or responsibility for the events giving rise to the proceedings or for the conduct of the litigation, expressly including those who have left. Not every employee, and not the or g an is at i on in some abstract sense: the census exists to name the actual list, and reasonable inquiry of those people (leavers included) is how a company per form s a duty framed around awareness.

Do we have to go looking for adverse documents?

The duty is framed around known documents, not a freestanding search obligation. But knowledge must be assembled honestly: asking the people whose awareness counts, running ordered searches neutrally, and not averting eyes from the obvious repositories. A party that structures its process to avoid acquiring knowledge invites the inference that it knew the knowledge was there to avoid, which is a worse position than the documents themselves.

What if the adverse document is privileged?

Genuinely privileged documents (legal advice, litigation work product) are not disclosable, adverse or otherwise, and the duty does not override privilege. The care point is precision: the damaging business document is not privileged because a lawyer later advised on it, and forwarding something to legal does not immunise it. Separate the original from the advice, take the decision deliberately, and record it.

We have just found something bad, late in the case. Now what?

Preserve it exactly as found, escalate to supervising counsel the same day, assess it soberly (authenticity, completeness, context, whether truly adverse), check privilege precisely, disclose promptly with such context as fairness allows, and record the chronology of when it became known and what was done. Late-arising knowledge, disclosed promptly, is the regime working; the only unrecoverable versions of this story involve delay or deletion.

How does this play in criminal and regulatory matters?

The same moral structure with sharper edges: CPIA 1996 obliges disclosure of material undermining the prosecution or assist in g the defence, investigators must pursue reasonable lines of enquiry away from as well as toward a suspect, and regulators expect candour about damaging material in responses and self-reports. The three pillars translate directly, and the documentation habit (methodology described, inquiries logged) is if anything more valuable where the sanctions are personal.