Locked Mobile Devices

Locked mobile devices present a strategy problem with a technical component. This guide details preservation, access routes, and legal authority, including s.49 RIPA. It covers risk management, common mistakes, and when to involve a digital forensic expert, offering a parallel-tracks framework for practitioners.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/locked-mobile-devices

LOCKEDMOBILEDEVICES · A GUIDE FOR UK LAWYERS Locked Mobile Devices Preservation, Access Routes, Legal Authority and the Decisions That Must Be Made Before Anyone Tries the Passcode COMPUTER FORENSICS LAB DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES LOCKED-DEVICE ASSESSMENT LAWFUL ACCESS & ENSEMBLE STRATEGY CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the wall that is some time s a door 03 First decisions: state, custody and the things nobody must do 04 The access routes, ranked by realism 05 Legal authority: consent, contract, compulsion and s.49 RIPA 06 Risk management: attempts, biometrics, lockouts and wipes 07 Strategy: the parallel-tracks framework 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: ALOCKEDDEVICEISASTRATEGYPROBLEMWITHATECHNICAL COMPONENT, ANDTHESTRATEGYHASPARALLELTRACKS

§ 02 · FIRST PRINCIPLES The problem in plain English: the wall that is some time s a door

§ 03 · HOURONE First decisions: state, custody and the things nobody must do

§ 04 · THEROUTES The access routes, ranked by realism ROUTE REALISM · WHAT GOVERNS IT

§ 05 · AUTHORITY Legal authority: consent, contract, compulsion and s.49 RIPA

§ 06 · NOTBREAKINGIT Risk management: attempts, biometrics, lockouts and wipes

§ 07 · THEPLAN Strategy: the parallel-tracks framework

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE LOCKED HANDSET CLOUD COMPUTER PAIRED COUNTERPARTS / DELETED / (IF ACCOUNT BACKUPS COMPUTERS PROVIDERS RECOVERABLE OPENED)

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THECLAUSETHATOPENEDTHEPHONE

EXAMPLE2 · THEBFUWALLANDTHEENSEMBLETHATWENTROUNDIT EXAMPLE3 · THEREFUSALTHATTESTIFIED

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

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The locked-device checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can a court really order someone to hand over their passcode? How long should we keep a device we cannot currently open? Is it worth paying for exotic unlocking services? The custodian offers to unlock it himself and show us the messages. Acceptable? What if the device wipes itself during exam in at i on? Does a factory-reset device end the inquiry?

§ 14 · 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

Can a court really order someone to hand over their passcode?

In civil proceedings, courts order disclosure of access information where necessary to make imaging and disclosure effective, and meet refusal with adverse inference, costs and enforcement: Example 3's machinery. The criminal/regulatory sphere has section 49 RIPA's compelled-disclosure regime with penal teeth, operated by authorities under safeguards. Neither guarantees the code appears: what they guarantee is that refusal acquires a price, which is frequently enough.

How long should we keep a device we cannot currently open?

In preserved custody for the matter's life, reviewed at milestones: Example 2's eight-month frontier movement is not rare, and storage is cheap against the option it keeps open. The review discipline matters more than the duration: a dated re-check at each case stage, and a deliberate decision: not a default: if preservation is ever abandoned.

Is it worth paying for exotic unlocking services?

Frame it as the capability check frames it: what does this device, in this state, actually admit: at what cost, risk and lawfulness: against what the ensemble already delivers? Sometimes specialist access is decisive and proportionate; often the same spend on cloud process and counterpart collection answers the case faster. Beware unconditional promises and provenance-free tools: the access must be lawful, documented and explicable in a CPR 35 report, or it is a liability wearing a receipt.

The custodian offers to unlock it himself and show us the messages. Acceptable?

As a route to scoping conversations, perhaps; as evidence, no: the self-guided tour is uncontrolled (what was scrolled, what was deleted mid-demonstration, what the reading did to disappearing messages) and unrepeatable. The counter-offer is the protections package: examiner extraction, targeted scope, personal content filtered: which meets the legitimate concern behind the offer while producing evidence that survives challenge. Guide 117 details the password-free variants.

What if the device wipes itself during exam in at i on?

Planned exam in at i on makes this a managed risk, not a gamble: wipe-on-failure settings assessed before attempts, budgets that stop short of trigger counts, iso l at i on preventing remote commands, and: where risk remains: the ensemble collected first so the worst case is bounded. A wipe under uncontrolled amateur attempts is a catastrophe; under laboratory protocol it is a foreseen contingency with the evidence already banked else where.

Does a factory-reset device end the inquiry?

It ends the handset inquiry and starts two others: the ensemble reconstruction (guide 61's Example 3: cloud, backups, mirrors, counterparts routinely rebuild the estate) and the conduct inquiry (the reset's timing, from act i v at i on and account records, read against the duty chronology). Modern resets on encrypted devices are genuinely effective against recovery: which is exactly why the reset itself, dated, so often becomes the exhibit. cflab. u k · e-disc ove r y. u k