IOS Spyware Stalkerware And Mobile Compromise

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/ios-spyware-stalkerware-and-mobile-compromise

SPYWARE, STALKERWARE & COMPROMISE · A GUIDE FOR UK LAWYERSiOS Spyware, Stalkerware and MobileCompromiseWhen the Phone Itself Is the Weapon: Detecting Covert Surveillance, and theDuty of Care It DemandsCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMSAFET Y-LED, VICTIM-CENTRED APPROACH CPR PART 35 EXPERT REPORT SFULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: when the phone is the weapon03 How iOS devices are covertly surveilled04 Detecting compromise, and its limits05 Safety first: the duty of care06 Interpretation and honest limits07 Deployment: protecting the person, then the evidence08 Source architecture: where else the evidence lives09 Worked examples10 Common mistakes and technical limitations11 Questions to ask · Suggested wording12 Checklist and red flags · When to involve a digital forensic expert13 Frequently asked questions14 Glossary · References · Disclaimer · How a specialist laboratory can assist§ 01 · ORIENTATIONExecutive summarysurveilled through consumer stalkerware, the misuse of legitimate features like shared location and Find My,or rare sophisticated spyware, and this work carries an unusual duty of care, because victim safety comes beforeevidence-gathering.§ 02 · FIRST PRINCIPLESThe problem in plain English: when the phone is the weapon§ 03 · HOWDEVICESARESURVEILLEDHow iOS devices are covertly surveilledSTALKERWARE MISUSED FEATURES CONTROLLED SPYWARE (RARE) WIDER VECTORSACCOUNT§ 04 · DETECTINGCOMPROMISEDetecting compromise, and its limits§ 05 · SAFETYFIRSTSafety first: the duty of care§ 06 · INTERPRETATIONANDHONESTLIMITSInterpretation and honest limits§ 07 · DEPLOYMENTDeployment: protecting the person, then the evidence§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE FAMILY LINKEDTHE ICLOUD PHYSICAL / SAFET YPHONE ACCOUNT NETWORK CONSIDERATIONSHARING / PAIRED /SET UP DEVICES§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THE " SPYWARE " THATWASASHAREDLOCATIONEXAMPLE2 · SAFETYBEFORETHESCANEXAMPLE3 · THECLEANSCANTHATWASNOTAGUARANTEE§ 10 · WHEREITGOESWRONGCommon mistakes and technical limitationsCommon mistakesTechnical limitations§ 11 · INTERROGATORIES & DRAFTING AIDSQuestions to ask · Suggested wordingAsk your clientAsk the other side / in proceedingsAsk your e Discovery / forensic providerSUGGESTED WORDING · INSTRUCTIONFORASUSPECTED - COMPROMISEANA LY SIS§ 12 · QUICK CONTROLChecklist and red flags · When to involve a digital forensicexpertThe suspected-compromise checklistRed flagsWhen to involve a digital forensic expert§ 13 · COMMON QUESTIONSFrequently asked questionsMy client thinks their phone is being tracked. Where do we start?Is it usually sophisticated spyware?Why can't you just scan the phone and be sure?Should we just remove any monitoring we find?Can this evidence be used in proceedings?What if the abuser controls the Apple account?§ 14 ·

REFERENCEGlossarySources and authoritative referencesDISCLAIMER§ HOW A SPECIALIST LABORATORY CAN ASSISTWorking with Computer Forensics LabSpeak to a forensic examiner, not a salesperson.INSTRUCTTHELABNEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

My client thinks their phone is being tracked. Where do we start?

With their safety, before any exam in at i on (

Why can't you just scan the phone and be sure?

Because detection on iOS is genuinely limited (

Should we just remove any monitoring we find?

Not reflexively, because removal can escalate risk (