IOS Spyware Stalkerware And Mobile Compromise

This guide for UK lawyers explains how iOS devices can be compromised by spyware, stalkerware, or misused features. It covers detection, the critical duty of care for victim safety, and how to handle mobile evidence in such sensitive cases, including common mistakes and expert involvement.

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 LAWYERS iOS Spyware, Stalkerware and Mobile Compromise When the Phone Itself Is the Weapon: Detecting Covert Surveillance, and the Duty of Care It Demands COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM SAFET Y-LED, VICTIM-CENTRED APPROACH CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: when the phone is the weapon 03 How iOS devices are covertly surveilled 04 Detecting compromise, and its limits 05 Safety first: the duty of care 06 Interpretation and honest limits 07 Deployment: protecting the person, then the evidence 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 surveilled 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 before evidence-gathering.

§ 02 · FIRST PRINCIPLES The problem in plain English: when the phone is the weapon

§ 03 · HOWDEVICESARESURVEILLED How iOS devices are covertly surveilled STALKERWARE MISUSED FEATURES CONTROLLED SPYWARE (RARE) WIDER VECTORS ACCOUNT

§ 04 · DETECTINGCOMPROMISE Detecting compromise, and its limits

§ 05 · SAFETYFIRST Safety first: the duty of care

§ 06 · INTERPRETATIONANDHONESTLIMITS Interpretation and honest limits

§ 07 · DEPLOYMENT Deployment: protecting the person, then the evidence

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE FAMILY LINKED THE ICLOUD PHYSICAL / SAFET Y PHONE ACCOUNT NETWORK CONSIDERATION SHARING / PAIRED / SET UP DEVICES

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THE " SPYWARE " THATWASASHAREDLOCATION EXAMPLE2 · SAFETYBEFORETHESCAN EXAMPLE3 · THECLEANSCANTHATWASNOTAGUARANTEE

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

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask the other side / in proceedings Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORASUSPECTED - COMPROMISEANA LY SIS

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

§ 13 · COMMON QUESTIONS Frequently asked questions My 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 · 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 if the abuser controls the Apple account?

§ 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

Source: https://e-discovery.uk/library/ios-spyware-stalkerware-and-mobile-compromise. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.