OSINT Open Source Intelligence In Litigation

Open source intelligence (OSINT) involves gathering public data for litigation. This guide covers capturing, preserving, verifying, and attributing OSINT to ensure it is lawful and proportionate. It details the open sources, legal limits, deployment, and common mistakes, helping practitioners turn information into admissible evidence.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/osint-open-source-intelligence-in-litigation

OPEN - SOURCEINTELLIGENCE · A GUIDE FOR UK LAWYERS OSINT: Open-Source Intelligence in Litigation Public Data, Lawful Method and Evidence That Holds Up COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: public does not mean proven 03 What OSINT covers: the open sources 04 Capturing and preserving so it can be authenticated 05 Verification, corroboration and attribution 06 Legal and ethical limits 07 Deployment: asset tracing, due diligence and fact-testing 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 OSINT is only useful when the material is captured and preserved so it can be authenticated, gathered law full y and proportionately, and verified rather than assumed, turning information into evidence that holds up.

§ 02 · FIRST PRINCIPLES The problem in plain English: public does not mean proven

§ 03 · THEOPENSOURCES What OSINT covers: the open sources SOCIAL / WEB COMPANY PROPERTY REGISTERS DOMAIN / WEB

§ 04 · CAPTURE AND PRESERVATION Capturing and preserving so it can be authenticated

§ 05 · VERIFICATIONANDATTRIBUTION Verification, corroboration and attribution

§ 06 · LEGALANDETHICALLIMITS Legal and ethical limits

§ 07 · DEPLOYMENT Deployment: asset tracing, due diligence and fact-testing

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE OPEN REGISTRAR SHARED ACCOUNT LIVE PLATFORM / OTHERS' DEVICE / SOURCE RECORDS COPIES FORENSICS WE B DELETED / ARCHIVES SUPERSEDED

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEHOLIDAYPHOTOSTHATANSWEREDTHEINJURYCLAIM EXAMPLE2 ·

THEHIDDENNETWORKBEHINDTHECOMPANY EXAMPLE3 · THEFAKESCREENSHOTANDTHECLEANMETHOD

§ 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 (where relevant) Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORANOSINTG AT HERINGANDANA LY SIS

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

§ 13 · COMMON QUESTIONS Frequently asked questions If information is public, can we just use it? Why is a screenshot not good enough? Can we set up a fake profile to see a private account? How do we know a social-media account belongs to the person? Can OSINT expose fabricated evidence? Is OSINT a substitute for disclosure and forensics?

§ 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

If information is public, can we just use it?

Gather it law full y, yes, but two cautions apply (§5, §6). First, public does not mean proven: open material is often wrong, stale or fabricated, so it must be verified, dated, attributed and corroborated before it is relied on. Second, gathering and using personal data still engages the UK GDPR and must be lawful and proportionate, and the gathering must stay within access laws and platform terms. Public material is a starting point for evidence, not evidence in itself.

Why is a screenshot not good enough?

Because it proves almost nothing on its own (§4, Example 1). A screenshot can be edited or fabricated, carries no reliable date, and has no verifiable link to a real source. Properly captured OSINT records the live URL, the page source, timestamps and metadata, is hashed, and its method is documented, so its authenticity and its state on the capture date can be proved. That is the difference between evidence that holds and an image that is challenged away.

Can we set up a fake profile to see a private account?

No (§6). Creating fake profiles to befriend or deceive a subject, logging into others' accounts, or circumventing access controls is unlawful or unethical, taints any evidence obtained and exposes the practitioner. OSINT works with genuinely public material gathered by honest means. Where information sits behind access controls, it is obtained by lawful process, disclosure, orders, not by deception or unauthorised access. The line is firm: public means public.

How do we know a social-media account belongs to the person?

By corroboration, not assumption (§5). Accounts are impersonated, shared and fake, so a name or photo is not enough. Attribution is built from corroborating evidence, consistent details across posts, connections, reused handles, and, where available, device and account forensics linking the account to the person (guides 105, 126). The honest position is stated: the account is attributed to the person where the evidence supports it, and left unattributed where it does not.

Can OSINT expose fabricated evidence?

Yes, and it often does (Example 3, §5). Fabricated screenshots of posts or messages are common, and verification, checking the platform's own records and web archives, testing the account, and apply in g provenance analysis (guide 126), frequently shows that the supposed material never existed. OSINT cuts both ways: it gathers genuine public evidence and it exposes fake public evidence, provided it is done with the same verification discipline in both directions.

Is OSINT a substitute for disclosure and forensics?

No, it complements them (§7, §8). OSINT is often the fastest way to learn something and to find where formal evidence lies, but public material is unverified and limited, so it points to the disclosure to seek, the account to have attributed, the asset to trace, while the authenticated capture, platform disclosure and device forensics supply the proof. Used together, OSINT and the forensic and disclosed sources are far stronger than either alone. cflab. u k · e-disc