WALDREP COMPANY CHECKLIST

Attorney Digital Evidence Checklist

AUDIENCE	Attorneys and litigation paralegals working a case with digital evidence — devices, cloud data, email, social media, or ESI.
PURPOSE	A pre-engagement checklist to make sure nothing is overlooked before evidence is lost, spoliated, or rendered inadmissible.

Section 1 — Preservation (do this first, even before retaining an expert)

- Send preservation letters to all opposing parties identifying specific custodians, devices, and accounts.
- Issue a litigation hold to your client covering email, text messages, cloud storage, social media, collaboration tools (Slack, Teams), and any work-issued or BYOD devices.
- Identify auto-delete settings (email retention, Slack message retention, ephemeral apps) and disable them in writing.
- Document the chain of custody from the moment any device or media is collected — date, time, who handled it, and where it was stored.
- Photograph devices in their original state before powering them off or moving them.

Section 2 — Scoping the evidence

- List every custodian whose data is potentially relevant.
- List every device, account, and platform per custodian (work phone, personal phone, laptop, iCloud, Gmail, Dropbox, work Microsoft 365, etc.).
- Identify the date range that is actually relevant to the matter — overly broad scopes drive cost without adding value.
- Identify any encryption, MDM, or remote-wipe risk (corporate iPhones can be wiped by the employer after termination).
- Confirm whether any data lives only with a third party (cloud provider, employer, ISP) and may require a subpoena or preservation request to that party.

Section 3 — Before you retain an expert

- Confirm the expert is court-qualified in the relevant jurisdiction and has never been disqualified.
- Confirm their methodology is peer-reviewed and Daubert/Frye defensible.
- Confirm they carry professional liability insurance.
- Confirm certifications relevant to the evidence type (Cellebrite, Magnet, EnCase, GIAC).
- Get a written engagement scope, hourly rate, and estimated budget before work begins.

Section 4 — During the engagement

- Require write-blocked, forensically sound acquisition — never analysis on the live device.
- Require hash values (MD5 or SHA-256) for every acquisition and verify the hash matches at every transfer.
- Ensure the expert's working copy is separate from the original evidence.
- Get interim updates in writing, not just verbally.

Section 5 — Before producing or relying on findings

- Confirm every assertion in the expert report is supported by an exhibit or extracted artifact.
- Confirm the report identifies tool versions, dates of analysis, and any limitations of the analysis.
- Have the expert walk you through the strongest opposing argument before opposing counsel does.
- Confirm metadata is preserved in any production — printing screenshots strips it.

About The Waldrep Company. Eric Waldrep is a court-qualified digital forensics expert with 17 years in forensics and 27 years in law enforcement. 200+ cases, 100% qualified, never disqualified. Federal and state court experience.

Need help on a specific matter? Schedule a free consultation at thewaldrepcompany.com/contact or call (251) 216-1164.