

Feel free to use as is or amend to suit your firm

The Silent Extraction Audit

This is a Vulnerability Assessment. Most lawyers believe that if they don't click an "AI Assistant" button, their data is safe. With increasing speed, the "SaaS Pivot" means AI is now the invisible engine under the hood of every standard office tool.

Use this audit to expose the "leaky pipes" in your firm's current workflow.

Section 1: The "Invisible" Email Engine

- Predictive Ingest: Does your email client (Gmail/Outlook) offer "Smart Reply" or "Summary" features? These functions require an LLM to "read" the entire body of your privileged communications on a third-party server to predict your next sentence.
- Metadata Harvesting: Is your provider "anonymizing" your metadata (who you talk to, how often, and subject line trends) to train their regional traffic models?
- Attachment Scanning: Does your email search function allow you to "Search inside PDFs"? If so, that indexing is likely happening in a multi-tenant cloud environment where "Confidentiality" is a contract, but not a physical reality.

Section 2: The PDF "Analysis" Trap

- Liquid Mode / Auto-Tagging: Tools like Adobe now use AI to "re-flow" or "tag" documents for accessibility. This requires the software to parse the semantic meaning of your legal briefs.
- Forced Cloud-Sync: Does your PDF editor require you to upload a file to their "Document Cloud" before it can run an OCR or a Redaction? Once it hits their cloud, the Heppner "Expectation of Privacy" is functionally compromised.
- Sidecar AI: Does your PDF reader have a "Chat with this Doc" sidebar? Even if you don't use it, is the software "preparing" the document for AI interaction the moment you open it?

Section 3: Storage & "Discovery" Leakage

- Smart Search / Insights: Does your cloud storage (Dropbox/OneDrive/GDrive) provide "File Insights" or "Suggested Folders"? This means an algorithm is constantly clustering your files based on their content.
- Third-Party Indexing: Many cloud storages use third-party sub-processors (like OpenAI or Amazon Bedrock) to generate thumbnails or "Smart Previews" of your evidence files.
- Revision History Logs: Are your "Deleted" files actually purged from the vendor's backup "Training Buckets," or do they persist in a "Safe-Learning" cache for 30–90 days?

Feel free to use as is or amend to suit your firm

Section 4: Communication & Transcription

- The "Always-On" Listener: Does your conferencing tool (Zoom/Teams) have a "Meeting Summary" feature enabled by default? If a bot is "listening" to transcribe, you have a third party in the room.
- Sentiment Analysis: Are your recordings being used to "improve voice recognition" or "analyze speaker sentiment"? This is a direct extraction of the emotional and strategic nuances of a client deposition.
- Background Noise Filtering: Modern "AI Noise Removal" often sends a digital fingerprint of the audio to a cloud model to "clean" the sound.