AI + PRIVILEGED COMMUNICATIONS CHECKLIST

General counsel, CISOs, and IT leadership can use the following checklist to evaluate AI integrations that may access privileged or confidential communications. This checklist is designed to be shared directly with IT and security teams for implementation.

1. Inventory and Authorization

□ Identify all AI applications and plug-ins deployed or available to employees
□ Map which repositories each AI application can access (Messages, email, cloud storage, collaboration tools, CRM, DMS)
□ Determine whether integrations require enterprise approval or can be enabled by individual users
□ Classify AI tools as Approved for Privileged Information / General Business Only / Not Approved

2. Data Flow and Processing

□ Document whether processing occurs on-device, in enterprise environment, or in provider's cloud
□ Identify what specific data is retrieved for each task type (search, summarization, drafting)
□ Confirm what data crosses device/network boundaries and under what circumstances
□ Verify whether subprocessors or third parties receive any data

3. Retention, Training, and Secondary Use

□ Confirm whether prompts, retrieved content, or outputs are retained by the provider
□ Document the applicable retention period and whether it is configurable
□ Verify whether customer data may be used for model training or improvement
□ Determine whether human reviewers may access customer content
□ Confirm data deletion rights and procedures

4. Contractual and Account Protections

□ Identify applicable terms (consumer ToS, enterprise agreement, DPA, BAA)
□ Confirm account type in use (consumer, business, enterprise) and verify applicable privacy commitments
□ Review confidentiality, security, and indemnification provisions
□ Determine data processing location and applicable data protection laws

5. Derivative Artifacts and Litigation Readiness

□ Identify what logs, summaries, chat histories, or other artifacts are created
□ Document where derivative artifacts reside and how they can be preserved or collected
□ Update litigation hold procedures to address AI-generated materials
□ Assess discoverability of AI interactions and outputs

6. Policy and Employee Controls

□ Update acceptable use policy to address AI integrations with messaging and communications
□ Establish clear prohibition on AI access to attorney-client communications without Legal/IT approval
□ Update BYOD policy to address personal AI accounts on devices containing company communications
□ Communicate AI policy to employees handling privileged, regulated, or confidential information
□ Implement technical controls where possible to restrict unauthorized AI integrations

Shumaker