Fisher Phillips

INVESTIGATIONS AND ATTORNEY-CLIENT PRIVILEGE IN THE AGE OF AI & MODERN COMMUNICATION PLATFORMS

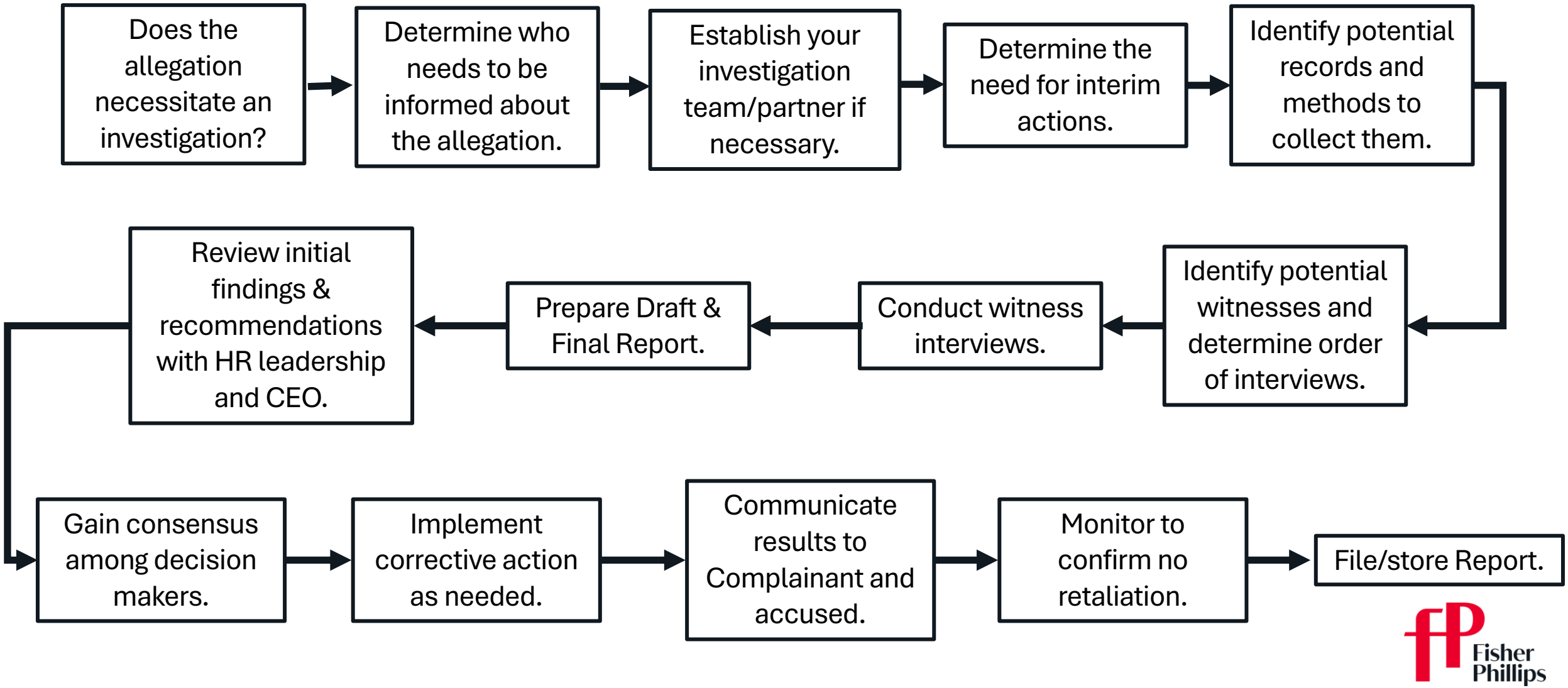


TERRI STEWART

Fisher & Phillips LLP
1230 Peachtree Street
Suite 3300
Atlanta, Georiga 30309
(404) 240-4247
tstewart@fisherphillips.com

Regional Managing Partner, Atlanta and Birmingham

Investigation Overview



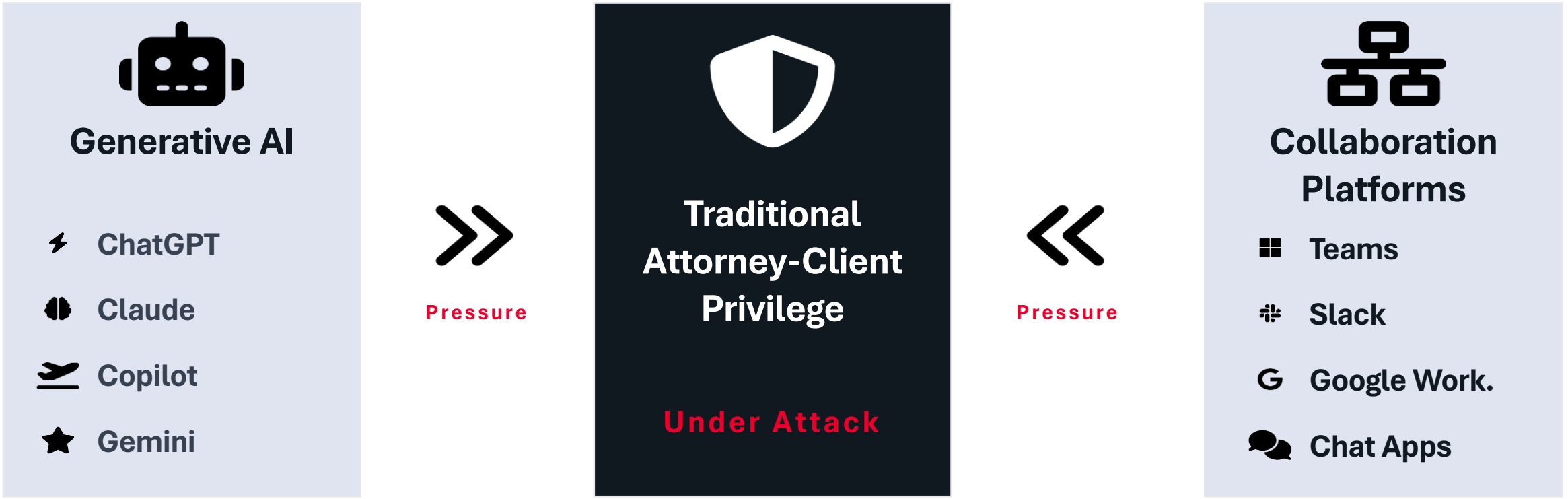
Fisher Phillips

Conducting Workplace Investigations

Program Overview

Part One – Overview and Pre-Investigation Considerations	Part Two - Planning & Conducting the Investigation	Part Three –Documenting & Concluding the Investigation
Overview • Why investigate • When to investigate • Who should investigate **Pre-Investigation Considerations** • Notifications • Attorney-Client Privilege • Interim Actions • Third-Parties • Off-Duty & Criminal Conduct	**Preparing the Plan** • Developing an Investigation Plan • Pre-interview investigation **The Interviews** • Conducting witness interviews	**Reaching Conclusions** • Assessing credibility • Making factual findings **The Written Report** • Drafting investigation report • Deciding on corrective action • Closing investigation • Post-investigation considerations

The Privilege Pressure Points



"The tools your employees use every day may be destroying your privilege protections without anyone realizing it."

Privilege 101 — The Three Elements

1



Between a client and an attorney (or attorney's agent)

2



Intended and kept confidential

3



For the purpose of seeking or providing legal advice

Crucial Note: The privilege belongs to the client — and the client can waive it.

In-House Context: Counsel face heightened scrutiny — the "primary purpose" test applies.

The Work-Product Doctrine



Protects materials prepared **"in anticipation of litigation"** by a party or its representative.



Broader than privilege — covers attorney mental impressions, theories, and strategy.



Waiver requires **disclosure to an adversary** (not just any third party).



Critical Distinction

The "to whom" standard for waiver is different from attorney-client privilege. Disclosure to a non-adversary third party does not necessarily waive work-product protection.

The February 10, 2026 Earthquake

Two Courts, Two Answers

FEB 10, 2026

Heppner

S.D.N.Y. (New York)

No Privilege
No Work Product

AI treated as third-party disclosure

Waiver of protection

"Functional equivalent" test failed

Warner

E.D. Mich. (Michigan)

Work Product Protected

AI treated as a "tool"

No waiver to adversary

Mental impressions preserved

Key Question

Is AI a "third party" or a "tool"?

United States v. Heppner

The Facts

Criminal defendant used **consumer Claude AI** independently.

Generated **31 documents** summarizing case strategy.

Subsequently **shared results with counsel**.

Three Privilege Failures

1 **Not an Attorney**
Claude is an AI tool, not a legal representative.

1 **No Confidentiality**
No reasonable expectation of privacy under Anthropic's consumer policy.

1 **No Direction**
Not made at counsel's direction for the purpose of legal advice.

The Waiver Bombshell

"Inputting privileged info into consumer AI = waiver of underlying privilege"

The Opposite View — Work Product Protected

Warner v. Gilbarco

Case Facts

Pro se plaintiff used **ChatGPT** for employment litigation preparation.

Employment Law Connection

Warner was an **employment discrimination** case, making this ruling particularly relevant for HR and employment counsel.

The Court's Key Holdings

AI Status

AI tools are ***"tools, not persons."***

No Waiver

Work-product waiver requires disclosure ***"to an adversary."*** Using AI privately does not waive protection.

Mental Impressions

Protected as ***"internal mental impressions reformatted through software."***

Why the Split Matters for Your Organization

Core Issue	Heppner (S.D.N.Y.)	Warner (E.D. Mich.)
Is AI a "Third Party"?	**YES** (Waiver Risk)	**NO** (It's a Tool)
Work Product Protected?	**NO**	**YES**
Privilege Status	**Waived** by disclosure	**Preserved** as mental impressions
Deciding Factor	Consumer Terms of Use & Lack of Confidentiality	Nature of use as a preparatory tool

No Precedent

No controlling precedent exists yet — both are district court decisions.

Prudent Approach

Assume AI is a **third party** until the law settles. Act conservatively.

Distinguishing Factors

Protected use requires: **Attorney direction**, enterprise tools, and purpose.

Consumer AI vs. Enterprise AI — The Critical Line

Consumer AI

- May **train on your data** to improve models
- Broad terms allow disclosure rights
- No Data Processing Addendum (DPA)

Likely destroys privilege per Heppner

The Critical Line

Enterprise AI

- **No-train commitments** (Data stays yours)
- Commercial Data Processing Addendum (DPA)
- Tenant isolation & SOC2 compliance

Stronger but untested privilege argument

"Consumer AI tools include the free and individual paid tiers of Claude, ChatGPT, Google Gemini, Microsoft Copilot, and Grok."

— Duane Morris

Concrete Example

Microsoft 365 Copilot (Enterprise)
Protected **vs** Copilot Free/Pro (Consumer)
Risky

The AI Privilege Checklist

1



Use Enterprise-grade tools with negotiated confidentiality terms & DPA.

2



Work performed at the direction and oversight of legal counsel.

3



Explicitly document the purpose as facilitating legal advice.

4



Label outputs as "Attorney-Client Privileged" or "Work Product".

5



Strictly restrict access to those within the privilege circle.

ABA Formal Opinion 512 — The Ethics Framework

Key Ethical Duties for AI Use

- **Competence**
- **Confidentiality**
- **Communication**
- **Candor**
- **Supervision**
- **Fees**

Critical Requirements

Informed consent required — **boilerplate is NOT enough**. You must explain the risks.

Self-learning tools: Must obtain client consent *before* inputting any client information.

Lawyers must understand how AI uses data and put **adequate safeguards** in place.

Collaboration Platforms

Email Era

Formal, asynchronous, clearly documented threads.

Chat Platforms

Teams, Slack. Rapid, informal, mixed business.

AI-Enhanced

Copilot, Agents. Auto-summaries, proactive generation.

Discoverable Records

Each platform creates permanent, discoverable records. What feels like a "hallway chat" is now evidence.

Increasing Scrutiny

Courts and regulators are increasingly seeking disclosure of informal chat logs and AI outputs.

The Core Conflict

Informal Culture + **Formal Laws** = **RISK**

Lessons from the OpenAI Slack Litigation

The Context

OpenAI established a specific Slack channel at their General Counsel's direction solely for the purpose of seeking legal advice.

The Court's Ruling

"No blanket channel privilege — each message must be evaluated individually."

Business discussions ≠ privileged just because counsel is a member of the channel.

What Was Protected

- Messages explicitly memorializing prior legal advice received from counsel.
- Counsel's specific legal concerns regarding AI risks and compliance.

What Was NOT Protected

- Messages between non-legal employees without specific legal content.
- Spreadsheets or attachments with only passing references to counsel.

Microsoft Teams — The eDiscovery Challenge

Data Architecture Reality



Exchange Online

1:1 Chats
Group Chats
Channel Messages

SharePoint/OneDrive

Channel Files
Shared Documents
OneNote

Note: Private Channels create separate Site Collections & Mailboxes

Legal Hold Gaps

CRITICAL RISK

- Holds are fragmented. User holds do **not** cover Channel or Private Channel content.
- **User Hold ≠ Channel Hold**

Governance Blind Spots

- Guest users and external collaborators access files and chats outside retention policies.
- Who controls joint data?

"Dark Data"

Context hidden in metadata:

- Emoji reactions (👍 = approval?)
- Edited/Deleted message logs
- Presence data & read receipts

Retention Settings

- Default settings are dangerous.
- **If unconfigured:** Content may be retained indefinitely (cost) or auto-deleted too soon (spoliation).

AI Transcription — The Silent Privilege Killer

Critical Risk Warning

Automated tools are creating discoverable records of privileged conversations without user awareness.

Technology Exposure

- Meeting transcription tools (Teams, Zoom, Otter.ai) are now **enabled by default** in many organizations.
- Every privileged conversation that's recorded automatically becomes a **discoverable record**.
- Third-party transcription services may store data externally and use it for **model training**.

Legal & Consent Risks

- **Wiretapping Statutes:** Recording without consent is a felony in some jurisdictions.
- **All-Party Consent Required:** PA, CA, FL, IL, MD, MA, MI, MT, NH, WA.
- Inadvertent waiver of privilege due to third-party presence (the AI bot).

Risk Management Best Practice

Turn AI transcription "OFF" by default; implement explicit prohibition for privileged conversations.

The Microsoft Copilot Permissions Problem

Security Gaps

- **Copilot inherits user permissions** — it sees *everything* the user can access.
- Copilot outputs **don't inherit** source file security labels.
- Legacy "Everyone" permissions create open doors for AI discovery.

15%+

of business-critical documents are overshared in typical organizations

Risk Scenario



Non-Legal Employee

Asks Question



Microsoft Copilot

Crawls Data



Over-permissioned SharePoint

Surfaces



Privileged Memo Exposed

The Solution | ✓ Data Partitioning ✓ Permission Audits ✓ Sensitivity Labels ✓ DLP for Copilot

The 2025 Federal Rules Amendments — Privilege Moves Forward

FRCP Rules 26 and 16 Amended

Effective Dec. 1, 2025

Early Conference

Privilege handling must be addressed at the initial **Rule 26(f) conference.**

Day 1 Priority

Privilege is no longer an 11th-hour issue — it is a **Day 1 priority** for all counsel.

Claw-Back Orders

Rule 502(d) orders are now considered **"Essential infrastructure"** for AI-era litigation.

Practical Impact

Every litigation plan must now account for AI and collaboration platform privilege from the outset.

Building Your AI Privilege Policy — Five Pillars

1

Ban Consumer AI

Zero Tolerance

Strictly prohibit the use of free, public AI tools for any client work.

- No ChatGPT Free
- No Claude / Gemini
- Name prohibited tools

2

Enterprise Governance

Deploy & Secure

Use only vetted enterprise solutions with strong contractual protections.

- ✓ Signed DPAs
- ✓ "No-Train" Commitments
- ✓ Full Audit Trails

3

Attorney Direction

Counsel Oversight

All AI usage for legal matters must be at the specific direction of counsel.

- Document purpose
- Review all outputs
- Validate accuracy

4

Partition & Protect

Isolate Data

Technical segregation of privileged content from general business data.

- Separate Legal Channels
- Restricted Permissions
- Sensitivity Labels

5

Train Everyone

Continuous Ed.

Comprehensive training program for all stakeholders, not just legal.

- Legal Staff & Execs
- Business Partners
- Annual Refreshers

Collaboration Platform Best Practices

- Clearly name and pin privilege language in legal channels
- Treat each message as potentially subject to individual review
- Moderate membership with counsel oversight
- Conduct regular permission audits
- Label every privileged communication
- Implement Rule 502(d) orders in all litigation as standard practice
- Disable auto-recording and AI transcription by default

Proactive Governance

The Client Counseling Imperative

Employees are the biggest risk vector — they often don't know what destroys privilege.

I asked ChatGPT to explain what our lawyer's email means.

Potential Privilege Waiver

I uploaded the investigation summary to get Copilot to draft a response.

Potential Privilege Waiver

I discussed our legal strategy in a Teams channel with 50 people.

Likely Waiver (Over-Sharing)

The AI note-taker recorded our call with outside counsel.

Discoverable Record Created

Training must be practical, scenario-based, and recurring.

What's Next — The Unsettled Landscape

As AI technology evolves faster than the legal system, organizations face significant uncertainty in these six key areas.



Judicial

No appellate court has ruled on AI and privilege.



Litigation

The Heppner/Warner split will likely deepen before it's resolved.



Corporate

Enterprise AI privilege arguments remain untested.



Ethics

State ethics opinions continue to proliferate.



Procedure

The 2025 FRCP amendments will generate new privilege jurisprudence.



Legislation

Potential legislative action on AI confidentiality.

Key Takeaways

01

Consumer AI tools are the most dangerous privilege risk your employees face today.

02

Collaboration platforms require message-level privilege discipline — no blanket protections.

03

AI transcription must be controlled with the same rigor as document classification.

04

Enterprise AI tools are necessary but not sufficient — governance and attorney direction are what matter.

05

Privilege strategy must begin on Day 1 of every matter (2025 FRCP amendments).

06

The law is developing rapidly — what's safe today may not be safe tomorrow.

QUESTIONS?

Fisher Phillips

THANK YOU