



2026 Product Liability & Complex Torts Practice Group Seminar September 16-18, 2026

**The Duty to Preserve & Protect
in an Age of Exploding Amounts of Data**
Legal Holds, Modern Data Sources, and Spoliation Risk

DAVID WARNICK

Moderator

JOHNSON & BELL, LTD.

Chicago, Illinois

warnickd@jbltd.com

BRETT CREASY

President and Director of Digital Forensics

BIT-X-BIT

Pittsburgh, Pennsylvania

brett.creasy@bit-x-bit.coM

JOHN UNICE

Chief Executive Officer

BIT-X-BIT

Pittsburgh, Pennsylvania

john.unice@bit-x-bit.com

WOODS PARKER

HUIE, FERNAMBUCQ & STEWART, LLP

Birmingham, Alabama

wparker@huielaw.com

JAY THOMPSON

MURPHY & GRANTLAND, P.A.

Columbia, South Carolina

jay.thompson@murphygrantland.com

I. When the Duty Attaches and What It Reaches

The Trigger

The duty to preserve evidence does not begin when a party files a lawsuit. It begins when a party knows or should know that evidence may be relevant to future litigation.¹ Courts call this the reasonably foreseeable standard. The standard is objective. The question is not whether the party actually expected litigation. The question is whether a reasonable party in the same position would have expected litigation.²

Common Trigger Events

Several events start the duty. Each of the following can make litigation reasonably foreseeable:³

- A demand letter that threatens litigation.
- A written request to preserve evidence.
- A direct verbal or written threat of litigation.
- The party's own decision to pursue a claim.
- Knowledge of an accident or incident that is likely to result in a claim.
- The filing of an administrative charge, such as a charge before the Equal Employment Opportunity Commission, or some other type of agency.

What Reasonably Foreseeable Means

A dispute alone does not always mean litigation is reasonably foreseeable, so the duty exists somewhere between knowledge of a dispute and a specific threat of suit.⁴ The test is flexible and fact specific. It lets a court examine each situation on its own facts.⁵ A potential claim alone does not start the duty. The standard does not require that litigation be imminent or probable.⁶

When Routine Destruction Is Not Spoliation

Standard operating procedures do not violate the duty if the party had no notice. Examples include the recycling of backup tapes and the overwriting of recorded data. If a party had no warning of future litigation, and no reason to believe the deleted information was relevant, routine destruction does not support sanctions.⁷

Scope: Documents and Electronically Stored Information

Once the duty attaches, the party must preserve all relevant documents and electronically stored information (ESI) in the party's possession, custody, or control.⁸ The scope covers information that is relevant and proportional to the claims and defenses in the case.⁹ Federal Rule of Civil Procedure 34 defines discoverable material broadly. It includes writings, drawings, graphs, charts, photographs, sound recordings, images, and other data compilations stored in any medium from which information can be obtained.¹⁰

Modern Data Sources

The definition reaches far beyond email and network file shares. Counsel must consider the following sources in every matter:

- Enterprise collaboration systems, such as Microsoft Teams, Slack, Google Workspace, and Quip.
- Messaging services (e.g., WhatsApp, Signal, WeChat, iMessage, and Telegram)
- Mobile devices, including personal devices that employees use for business (BYOD).
- Cloud storage and software-as-a-service (SaaS) platforms.
- Data that a vendor stores on the client's behalf.
- Artificial intelligence tools, including prompts, outputs, uploaded files, and tool logs.

Possession, Custody, or Control

The duty reaches data in the party's possession, custody, or control.¹¹ An employee who uses a private messaging account or a personal email account for business can bring that account within the company's control. Examples include an employee who puts a private address in a work email signature, and an employee who installs messaging software on a work computer. In that situation, the company must preserve the data and provide access to it. **The absence of a policy that separates personal data from business data is not a defense.** A company that permits mixed use accepts the preservation burden that follows.

Duration and System Scope

The duty is continuous. It runs for the length of the litigation.¹² The duty applies to every location and every system that holds relevant data. This includes on-site servers and backup systems, off-site storage and cloud platforms, employee workstations and laptops, company mobile devices and personal mobile devices used for business, personal accounts used for business, vendor-controlled systems, and the data of departed employees.

Uncertainty About Scope at the Trigger

A trigger event often gives limited information. The party frequently does not know the precise claims, the parties, or the time period at issue. Counsel must scope preservation on incomplete facts. A detail that looks marginal at the trigger can become central later. In a premises case, for example, the length of time a hazard was present is often the decisive fact. Surveillance video from the hours before an incident can therefore be relevant even though the issue is not yet framed. Counsel should scope preservation to what a reasonable party could foresee at the time, and should document that reasoning contemporaneously.

II. Implementing a Legal Hold in a Complex IT Environment

A legal hold notice is the beginning of the discovery obligation. "A party's discovery obligations do not end with the implementation of a 'litigation hold' -- to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."¹³ Counsel cannot issue a notice, file it, and assume that custodians will comply.

Step 1: Learn the Retention Architecture

Counsel must learn the organization's document retention policies. Counsel must also learn the technical architecture that implements those policies.¹⁴ Counsel cannot rely on passive instructions and should not assume that employees have the technical knowledge to find and preserve electronic data.¹⁵

Step 2: Work Directly with Information Technology Personnel

Counsel must speak directly with information technology staff.¹⁶ Ineffective communication with information technology personnel is one of the primary reasons that electronic data is lost.¹⁷ IT personnel perform three functions that no one else can perform:

- They explain system-wide backup procedures.
- They explain how recycling and deletion policies operate in practice, which is often different from how the written policy reads.
- They separate relevant backup media and active files from the standard data pool.

The Duty to Preserve

Step 3: Apply Preservation at the Platform Level

A legal hold notice tells people not to delete relevant information. It does not configure enterprise systems to retain that information. These are two different actions. Counsel must complete both.

Microsoft 365 illustrates the point. The hold team must decide whether to create an eDiscovery hold in Microsoft Purview, and must decide which content locations the hold covers. Where an in-system hold is not available, the team should create a point-in-time preservation by collection. Microsoft documents that eDiscovery holds can preserve Exchange mailboxes and OneDrive accounts, and can preserve mailboxes and sites associated with Microsoft Teams, Microsoft 365 groups, and Viva Engage groups.¹⁸ The following steps apply:

- Identify the users, group mailboxes, Teams-related mailboxes, SharePoint sites, and OneDrive sites that hold potentially relevant content.
- Choose between an infinite hold and a query-based hold. Microsoft also documents date-range scoping for content sent, received, or created in a specified period.
- Verify licensing before you rely on a hold. Microsoft users require eligible licensing, and that some query-based, time-bound, and custodian-scoped features exist only in higher licensing tiers.
- Monitor the policy state. The hold dashboard reports states that include Draft, On, Off, In progress, and Pending deletion. Retry any policy that needs attention.
- Do not confuse long-term records retention with an eDiscovery hold. Microsoft directs organizations to retention policies and retention labels for long-term retention that is unrelated to an investigation.

The same discipline applies to every other platform in scope. Confirm the capability, apply it, and verify the result.

Step 4: Identify and Instruct the Key Players

Counsel must speak directly with the key players in the matter and must learn how each of them stores information.¹⁹ Counsel must take three actions:²⁰

- Provide clear written communications that explain the preservation duty.
- Instruct key players to produce electronic copies of their relevant active files.
- Identify the sources of potentially relevant ESI and the associated metadata.

Do not assume that every custodian understands the obligation. Some custodians misunderstand the notice. Some custodians never receive it.²¹

Step 5: Monitor Compliance

Counsel and management must take affirmative steps to oversee compliance.²² The following actions are necessary:

- Supervise the execution of searches directly.
- Do not delegate searches to unsupervised staff who do not know the email or storage systems.
- Search for and identify new sources of discoverable information as the case develops.
- Confirm that each relevant actor understands the hold and applies it for the full length of the case.

Step 6: Assemble a Hold Team and Track the Hold in a System

An organization should assemble a dedicated hold team. The team oversees, tracks, and documents compliance until the organization formally releases the hold. The team should include outside counsel, in-house counsel, management-level employees from the affected departments, and an IT employee who knows the systems, the

The Duty to Preserve

architecture, and the retention policies. The notice should name one point person who answers questions and coordinates with outside counsel.

Spreadsheet tracking becomes unreliable as the number of custodians, matters, reminders, questionnaires, and preservation actions grows. A dedicated legal hold platform centralizes the workflow. Relativity Legal Hold is one example. Its documentation describes a workflow that issues email notices, interviews custodians through questionnaires, follows up with unresponsive custodians, escalates unanswered notices to managers, tracks responses, and generates reports that maintain an audit trail.²³ A platform of this type gives four benefits:

- Standard notice, reminder, escalation, questionnaire, and release templates make repeat processes consistent.
- One system holds notices, acknowledgements, questionnaire responses, follow-up activity, and closure records.
- Reports and activity history document communications and exceptions.
- Some platforms connect to enterprise systems through an application programming interface (API) and instruct those systems to place data on hold.

Keep one distinction clear, that is, notification management is NOT technical preservation. A completed acknowledgement does not establish that anyone placed data on hold in Microsoft 365, in Slack, or in any other source.

Step 7: Consider an Outside Vendor

An organization should strongly consider an outside e-discovery vendor when a matter involves large volumes of ESI and metadata. A vendor assists with preservation, collection, and production, and creates a defensible record of the process.

Technical Triage After a Trigger Event

Meet with IT and other stakeholders as soon as possible after the trigger. Some systems have short retention windows. Some systems are not fully managed by IT. Both categories create immediate risk. Examples include BYOD mobile devices, where text messages are among the most requested sources; audit and security logs from enterprise systems and endpoints; and security camera footage. The systems that matter depend on the type of case:

- Products disputes: engineering systems (CAD drawings, including non-final versions), customer support and complaint databases (messages and call recordings), and regulatory records (submissions to bodies such as the FDA and NHTSA, including CAPA records and MDR reports).
- Sales disputes: customer relationship management systems, Teams, email, and call recordings.
- Employment disputes: human resource information systems, email, mobile devices, and text messages.
- Trade secret disputes: OneDrive, GitHub, engineering file shares, and SaaS applications.

Specific Challenge: Auto-Delete in Email and Messaging

Automatic deletion settings destroy evidence quietly. A party that continues to run an auto-delete email system after notice of potential litigation, and that fails both to suspend the function and to secure custodian compliance, acts in conscious disregard of its preservation duty.²⁴ Identify every auto-delete and auto-expiry setting in email, chat, and messaging platforms. Suspend each one. Record what you suspended and when.

The Duty to Preserve

Specific Challenge: Native CAD Files

Many people think of a CAD drawing as a static file, similar to a PDF. It is not. A CAD system frequently contains design history, assembly relationships, embedded metadata, material specifications, revision history, user attribution, and references to external files.

Preservation therefore requires more care than a simple file copy:

- Preserve the native CAD files in addition to any rendered output.
- Document the software version that created the design.
- Preserve linked assemblies and reference files.
- Preserve the associated database records.
- Capture user and revision metadata before any migration or upgrade.

Production of a PDF or TIFF image of a drawing can remove the evidence that matters most. The image does not show who made a change, when the change occurred, which dimensions changed, or what earlier versions existed.

Specific Challenge: Slack

Evaluate Slack as its own preservation system. Do not treat it as an extension of email. Slack publishes a dedicated administrative function for legal holds.²⁵ The technical team must confirm that the organization's Slack plan and administrative roles provide the required hold capability, identify the custodians in scope, and verify that the hold retains the relevant messages and files. Five steps apply:

- Inventory the workspaces, Enterprise Grid organizations, custodians, guest accounts, deactivated users, channels, direct messages, group messages, Slack Connect activity, and attached or linked files in scope.
- Document the workspace retention configuration and how the hold interacts with ordinary retention.
- Confirm whether preservation occurs natively in Slack, through an integrated hold platform, through a third-party archive, or by export to external retention.
- Test whether edited content, deleted content, file attachments, linked cloud documents, and deactivated-user content survive through the selected path.
- Record plan, permission, API, retention, and export limitations as preservation exceptions. Do not assume that a cloud service retains everything.

Specific Challenge: Enterprise Artificial Intelligence Activity

Enterprise AI services hold records that exist nowhere else. These include conversations, uploaded files, workspace configuration, memories, user records, and audit events. For ChatGPT Enterprise and Edu, OpenAI documents a compliance platform that supplies logs and metadata, and that connects to eDiscovery, data-loss-prevention, and security information and event management tools. OpenAI describes two access patterns: immutable append-only compliance logs, and a stateful API that queries current state and certain legacy audit data.²⁶ Four steps apply:

- Identify the workspace, the administrators, the users, the retention configuration, the enabled applications, and the relevant time period.
- Determine whether continuous export is necessary. OpenAI states that the compliance logs platform retains data for 30 days, and that longer retention requires the customer to download and retain the logs under its own policy.
- Map the available records to the hold scope. Categories include conversations, files, workspace GPT

The Duty to Preserve

configuration and metadata, memories, workspace users, administrative events, and authentication events.

- Do not assume that deleted source data is recoverable. OpenAI states that the compliance platform cannot recover deleted data.

Confirm what a connector actually captures against current vendor documentation. Feature sets in this area change quickly, and a static list becomes wrong within months.

Specific Challenge: Mobile Devices and BYOD

Rule 37(e) requires a party to take reasonable steps to preserve ESI.²⁷ A party that fails to back up the mobile devices of relevant employees, or that fails to suspend ordinary mobile data destruction policies, exposes itself to severe sanctions. Mobile preservation requires an early decision, because device turnover and message expiry destroy data quickly.

Questions to Ask Information Technology

Ask the following questions at the first triage meeting:

- Are the mobile devices company-owned or BYOD?
- Are the devices enrolled in mobile device management, and do those policies block collection?
- Are any relevant custodians former employees, and what procedures govern their accounts and devices?
- What systems do the identified custodians use as standard, which may require input from the custodian's manager rather than from IT?
- What non-standard systems do the relevant custodians use?

Counsel's Heightened Duty

The preservation obligation runs first to counsel. Counsel must advise the client about the types of information that are potentially relevant, and about the need to prevent destruction of that information. This responsibility is heightened in the age of electronic discovery.²⁸ Attorneys and clients must work together so that both understand how and where the client maintains electronic documents, records, and email. Attorneys must take responsibility for ensuring that the client conducts a comprehensive and appropriate search.

Common Failures

Preservation programs fail in predictable ways. The following failures recur across reported cases:²⁹

- District managers receive broad discretion to decide who receives a hold and what the hold covers.
- Managers must ensure that departing employees segregate and preserve documents, but no one verifies that they did.
- Employees choose their own method of segregating and storing relevant documents.
- The organization fails to keep backup media and fails to retain hard drives.
- Employees believe that documents left in an office or on a computer will be retained, while IT believes that it may wipe a hard drive once an employee departs unless someone makes a specific request.
- The organization continues to run auto-delete email after notice of potential litigation, and does not distribute or follow up on hold notices until after a plaintiff files suit.³⁰

III. Sanctions Under Rule 37(e) and the Cost of Getting It Wrong

The Two-Tier Framework

A court may impose sanctions under Rule 37(e) when three conditions are met. (1) ESI that should have been preserved is lost, (2) the party failed to take reasonable steps to preserve it, and (3) the data cannot be restored or replaced through additional discovery.³¹ Rule 37(e) then establishes a strict two-tier framework.³²

Curative Measures

If the court finds that the loss of ESI prejudiced another party, the court may order measures no greater than necessary to cure the prejudice.³³ This tier requires a finding of prejudice alone. It requires no finding of intent. Curative measures include additional discovery at the spoliating party's expense, preclusion of evidence or argument, and monetary sanctions that compensate for the cost of additional discovery.

Severe Sanctions

The court may impose severe sanctions only on an explicit finding that the party acted with the intent to deprive another party of the information's use in the litigation.³⁴ Severe sanctions include an instruction that the jury may or must presume the lost information was unfavorable, a presumption by the court to the same effect, dismissal of the action, and entry of default judgment.

Intent to Deprive

The intent to deprive standard is equivalent to bad faith. It means the willful destruction of evidence for the purpose of preventing an adverse party from discovering it.³⁵ Negligence does not satisfy the standard. Gross negligence does not satisfy the standard either.³⁶ The 2015 amendments to Rule 37(e) expressly reject the cases that permitted an adverse inference instruction on a finding of negligence or gross negligence. Only an intentional loss supports the inference that the lost evidence was unfavorable to the party responsible for the loss.

Proving Intent with Circumstantial Evidence

Direct evidence of intent is rare. A court may therefore find intent from circumstantial evidence.³⁷ Courts weigh factors that include the following:

- The timing of the destruction.
- Affirmative steps taken to delete evidence.
- Selective preservation, or selective deletion of messages while surrounding communications survive.
- Use of data-wiping software, or an operating system upgrade run immediately before a scheduled forensic examination.
- The absence of any coherent explanation for a failure to suspend automatic destruction or to instruct custodians.
- Factual misrepresentations to the court about the state of preservation, made before anyone verified whether the data existed.

The last two factors deserve particular attention from defense counsel. Both describe process failures rather than deliberate destruction, and both are avoidable through documentation.

The Duty to Preserve

Prejudice and Inherent Authority

Gregory v. Montana, 118 F.4th 1069, 1072 (9th Cir. 2024), is a useful example. The case involved lost surveillance footage. The State knew it had to preserve the footage for the criminal case, and a later civil claim was foreseeable. That was enough to bring the footage within Rule 37(e). The problem was the sanction. The district court did not simply order a cure for prejudice. It imposed a conclusive adverse determination, which functioned like a severe sanction. For that level of relief, Rule 37(e)(2) required a finding that the State intended to deprive the other party of the footage for use in litigation. The record did not support that finding. The Ninth Circuit therefore held that the court could not use inherent authority to avoid Rule 37(e)'s limits.³⁸

Rule 37 more broadly authorizes a spectrum of sanctions for failures to obey discovery orders, and dismissal remains available in an appropriate case. The Supreme Court has held that the sanction must remain available not only to penalize the party whose conduct warrants it, but also to deter others.³⁹

Spoliation of Physical Evidence

Rule 37(e) does not reach physical evidence. For non-ESI, federal courts continue to apply common-law spoliation principles and may look to inherent authority.⁴⁰ The general standard requires a showing that the party with control over the evidence had an obligation to preserve it, that the party destroyed the evidence with a culpable state of mind, and that the destroyed evidence was relevant to a claim or defense.

A party that cannot preserve physical evidence because it does not own or control that evidence still has an obligation. It must notify the opposing party of access to the evidence, or of the possible destruction of it.⁴¹ In product liability practice this obligation arises constantly, because the allegedly defective product often sits with the plaintiff, an insurer, a repair facility, or a salvage yard.

The Risks of Under-Preservation

Under-preservation creates four categories of risk:

- Curative sanctions, which include additional discovery at the party's expense, preclusion of evidence or argument, and monetary sanctions.
- Severe sanctions, which include adverse inference instructions, a presumption that the lost information was unfavorable, dismissal, and default judgment.
- Evidentiary gaps. Even where a court imposes no sanction, the absence of the evidence weakens the defense at trial.
- Reputational harm. A finding of spoliation, and a finding of bad faith in particular, damages the party's credibility with the court, with the jury, and in later litigation.

The Risks of Over-Preservation

Over-preservation carries its own costs, and clients feel them immediately:

- Cost and burden. Storage costs, IT personnel time, legal review costs, and vendor costs all rise with volume.
- Increased discovery exposure. More preserved data means more discoverable data, longer review, higher cost, and greater risk of inadvertent disclosure of privileged or confidential material.
- Operational disruption. Employees lose normal deletion and filing practices, storage demand degrades system performance, and departing employees require additional exit procedures.

The Duty to Preserve

Balancing the Two Risks

The legal standard remains reasonableness and good faith. A litigation hold is not necessary in every circumstance.⁴² An organization should tailor preservation to the nature and scope of the anticipated claims, to the likely relevance of each data source, and to the proportionality of the effort against the stakes in the case. Rule 26(b)(1) supplies the proportionality factors. They are the importance of the issues at stake, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.⁴³

Inaccessible Data

A party need not ordinarily provide discovery of ESI from sources that are not reasonably accessible because of undue burden or cost.⁴⁴ On a motion to compel or for a protective order, the responding party bears the burden of showing that undue burden or cost. Even where the party makes that showing, the court may still order discovery on a showing of good cause.

This exception governs production. It does not govern preservation. A party must still preserve ESI that it should have preserved when the duty attached, whether or not the source is reasonably accessible.

IV. The Hold Notice: Privilege, Work Product, and At-Issue Waiver

No Automatic Privilege

A litigation hold notice is not automatically privileged. Protection depends on a case-by-case analysis of whether the notice satisfies the elements of the attorney-client privilege or the work-product doctrine.

The underlying facts about a party's preservation efforts are generally discoverable. The notice itself may still be protected if it is a confidential communication made to obtain or provide legal advice, or if the author prepared it in anticipation of litigation and it contains attorney mental impressions. A party must assert the protection document by document. A blanket assertion fails. The party that resists discovery bears the burden of establishing that the protection applies.

Attorney-Client Privilege

To protect a hold notice under the attorney-client privilege, the asserting party must show four elements:

- The document is a communication.
- The communication occurred between privileged persons, meaning the client, the attorney, and the agents of each who facilitate the representation.
- The parties made the communication in confidence.
- The primary purpose of the communication was to obtain or provide legal assistance or legal advice.

The privilege protects the communication. It does not protect the underlying facts. It protects instructions and legal advice that general counsel sends to employees about preservation duties. It does not prevent an opposing party from discovering the facts and data that those employees hold. Disclosure to a third party waives the privilege.

Work-Product Doctrine

Rule 26(b)(3) codifies the work-product doctrine.⁴⁵ To qualify, the proponent must establish that the hold notice is a document or tangible thing, that the author prepared it in anticipation of litigation or for trial, and that the

The Duty to Preserve

author prepared it by or for a party or a party's representative, including an attorney, consultant, or agent. Courts apply the because-of test to hold notices, because the prospect of a legal claim is what creates them. Under that test a document is protected if, given its nature and the factual situation, the author fairly prepared it because of the prospect of litigation, and would not have created it in substantially similar form but for that prospect. The doctrine does not cover documents prepared in the ordinary course of business.

Protection has two tiers. Ordinary work product, meaning the general information and facts compiled in the document, is discoverable if the requesting party shows a substantial need for the material and shows that it cannot obtain the substantial equivalent by other means without undue hardship. Opinion work product, meaning the mental impressions, conclusions, opinions, or legal theories of an attorney, receives nearly absolute protection. A court will compel it only in exceptional circumstances, where the mental impressions are the pivotal issue and the need is compelling.

Both protections are waivable. Voluntary disclosure of a meaningful part of a hold notice to a third party or an adversary may waive the protection. Under Federal Rule of Evidence 502, an intentional waiver in a federal proceeding may extend to undisclosed communications that concern the same subject matter and that fairness requires to be considered together.⁴⁶

The At-Issue Waiver Doctrine

A party may implicitly waive the attorney-client privilege or work-product protection by putting confidential information in controversy.

Protected communications do not become at issue merely because they are relevant, vital, or highly probative. The waiver rests on fairness and on the shield-and-sword principle. That principle prevents a litigant from relying on privileged information to prove a point while using the privilege to block the opponent from testing the assertion.

Courts apply a three-prong test.⁴⁷ An implied waiver arises only if the party seeking disclosure shows all three of the following:

- The assertion of the privilege resulted from an affirmative act by the asserting party, such as filing a claim or asserting an affirmative defense.
- Through that affirmative act, the asserting party put the protected information directly at issue and made it relevant to the case.
- Application of the privilege would deny the opposing party access to information that is vital to its claim or defense.

The overarching question is whether protection would be manifestly unfair to the opposing party. A waiver applies where the privilege holder makes assertions whose truth can be assessed only by examining the underlying privileged communications.

Application to Preservation Disputes

A party does not lose the privilege merely because the litigation places its state of mind, its intent, or its conduct in controversy. The privilege holder must affirmatively inject the privileged communications, or the advice of counsel, as an essential element of a claim or defense.

A party waives the privilege if it relies on the advice of counsel to establish the reasonableness of its conduct

The Duty to Preserve

while withholding the contents of that advice. A party also waives the privilege if it discloses part of the privileged information to support its position and then asserts the privilege over the remainder.

This distinction governs preservation disputes directly. When an opponent challenges preservation efforts over lost ESI, the court evaluates whether the party took reasonable steps.⁴⁸ A party may defend its conduct by showing that it acted in good faith and followed its policies. That defense does not waive the privilege by itself. The waiver arises only when the party relies on the specific substance of privileged communications to justify its preservation efforts.

The practical lesson is a drafting lesson. Build the defensibility record out of facts, dates, system configurations, and custodian actions. A party can prove those facts without opening the hold notice. A defense built on what counsel advised opens the notice.

V. State-Law Variations Counsel Must Confirm

The framework above is federal. Sections I through IV describe federal law and the Federal Rules of Civil Procedure. State practice diverges on six points that matter to a preservation program. Counsel should confirm the governing rule before scoping any hold, and national coordinating counsel should assume divergence rather than uniformity.

The Culpability Threshold for an Adverse Inference

Rule 37(e)(2)'s intent-to-deprive threshold is federal. Many states never adopted the 2015 amendment. Several state courts permit an adverse inference on a showing below bad faith. New York allows an adverse inference for the negligent loss of ESI, although the movant must prove the relevance of the lost material where the destruction was merely negligent rather than intentional or grossly negligent.⁴⁹ Texas moves in the opposite direction and requires intentional spoliation before a court may give a spoliation instruction, subject to a narrow exception where the non-spoliating party is irreparably deprived of any meaningful ability to present a claim or defense.⁵⁰

The Independent Spoliation Tort

Federal courts and most states reject an independent tort of spoliation and rely on evidentiary and discovery sanctions instead. A minority of states recognize the tort. New Mexico recognizes an intentional spoliation tort.⁵¹ Ohio recognizes a tort for interference with or destruction of evidence, although the Ohio Supreme Court later held that the tort requires physical destruction or alteration, and that concealment or misrepresentation alone is not actionable.⁵² California declines to recognize a freestanding spoliation tort against a party or a third party.⁵³ Florida illustrates the direction of travel. It once recognized a first-party claim and later rejected it in favor of sanctions and the rebuttable presumption.⁵⁴

The Control Test

Not every jurisdiction applies the federal possession, custody, or control standard identically. Some courts measure control by a party's legal right to obtain the data. Others apply a practical-ability test, which reaches material held by affiliates, vendors, or employees that a legal-right test would exclude.⁵⁵ The difference changes the scope of a hold. Confirm which test governs before you scope preservation, particularly where relevant data sits with a foreign affiliate or a third-party administrator.

The Duty to Preserve

The Scope and Form of ESI Production

State discovery regimes define discoverable ESI on their own terms. Texas requires a party to request electronic data specifically and to specify the form of production, and the Texas Supreme Court applies its own proportionality analysis that can diverge from Federal Rule 26(b)(1).⁵⁶ California's Civil Discovery Act governs ESI separately and sets its own procedure for objecting to production from sources that are not reasonably accessible.⁵⁷ A definition of documents or of electronically stored information may be narrower or broader than the federal standard.

Work-Product Protection

The privilege and work-product rules in Section IV are federal. In state court, work-product protection is frequently statutory and may be narrower or broader than Rule 26(b)(3). California grants absolute protection to a writing that reflects an attorney's impressions, conclusions, opinions, or legal research or theories, which is a stronger shield than the qualified federal standard.⁵⁸ The tests for at-issue waiver and implied waiver also vary. Confirm the governing rule before you rely on the privileged status of a hold notice.

A Practical Checklist

The following actions convert the preceding analysis into a defensible process:

- Document the trigger. Record what the organization learned, when it learned it, and who learned it.
- Convene IT and business stakeholders within days, not weeks. Start with the systems that have the shortest retention windows.
- Issue the hold notice, and separately apply preservation inside each platform. Verify the second step.
- Suspend every auto-delete and auto-expiry setting in scope, and record what you suspended and when.
- Name one point person and one hold team, and track acknowledgements in a system rather than a spreadsheet.
- Reassess scope as the case develops. Preservation is continuous, and new custodians and new systems appear.
- Build the defensibility record out of facts and system evidence, so that the record does not depend on the contents of privileged communications.
- Confirm the governing state rule on culpability, control, scope, and work product before you rely on the federal framework.

¹ *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011).

² *Bistran v. Levi*, 448 F. Supp. 3d 454, 468 (E.D. Pa. 2020).

³ *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 103-04 (E.D. Va. 2018).

⁴ *Id.*

⁵ *Bistran*, 448 F. Supp. 3d at 469-70.

⁶ *Id.*

⁷ *Turner v. United States*, 736 F.3d 274 (4th Cir. 2013).

⁸ Fed. R. Civ. P. 34(a)(1); see also Fed. R. Civ. P. 26(b)(1).

⁹ Fed. R. Civ. P. 26(b)(1).

¹⁰ Fed. R. Civ. P. 34(a)(1)(A).

¹¹ *supra* note 8.

¹² *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 431 (S.D.N.Y. 2004)(finding implementation of a litigation hold is not sufficient to comply with a party's duty to preserve evidence and that, instead, the party's attorney must also "take affirmative steps to monitor compliance".) **Author Note: This case was decided prior to Rule 37 amendment in 2015 when negligence or gross negligence permitted spoliation claim versus now where intent is required.**

¹³ *Zubulake*, 229 F.R.D. at 432.

¹⁴ *In re Ethicon, Inc. Pelvic Repair Sys. Prods. Liab. Litig.*, 299 F.R.D. 502 (S.D. W. Va. 2014).

¹⁵ *Scalera v. Electrograph Sys., Inc.*, 262 F.R.D. 162, 177-78 (E.D.N.Y. 2009).

¹⁶ *In re Ethicon*, 299 F.R.D. 502.

¹⁷ *Scalera*, 262 F.R.D. at 178.

¹⁸ Microsoft, Manage Holds in eDiscovery, Microsoft Learn, <https://learn.microsoft.com/en-us/purview/ediscovery-managing-holds> (last visited Aug. 26, 2026).

¹⁹ *In re Ethicon*, 299 F.R.D. 502.

²⁰ *Zubulake*, 229 F.R.D. at 433-34.

²¹ *In re Ethicon*, 299 F.R.D. 502.

²² *Scalera*, 262 F.R.D. at 177-78.

²³ Relativity, Legal Hold, Relativity Documentation, <https://help.relativity.com> (last visited Aug. 26, 2026).

²⁴ *Apple Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1143, 1149 (N.D. Cal. 2012).

²⁵ Slack, Manage Legal Holds, Slack Help Center, <https://slack.com/help> (last visited Aug. 26, 2026).

²⁶ OpenAI, Compliance API for ChatGPT Enterprise and Edu, OpenAI Help Center, <https://help.openai.com> (last visited Aug. 26, 2026).

²⁷ Fed. R. Civ. P. 37(e).

²⁸ *Telecom Int'l Am., Ltd. v. AT&T Corp.*, 189 F.R.D. 76, 81 (S.D.N.Y. 1999); accord *Green v. McClendon*, 262 F.R.D. 284 (S.D.N.Y. 2009).

²⁹ *In re Ethicon*, 299 F.R.D. 502.

³⁰ *Apple*, 881 F. Supp. 2d at 1149.

³¹ Fed. R. Civ. P. 37(e); *Paisley Park Enters., Inc. v. Boxill*, 330 F.R.D. 226 (D. Minn. 2019).

³² *Gregory v. State of Montana*, 118 F.4th 1078-79 (9th Cir. 2024).

³³ Fed. R. Civ. P. 37(e)(1); *Hoffer v. Tellone*, 128 F.4th 433, 437-38 (2d Cir. 2025).

³⁴ Fed. R. Civ. P. 37(e)(2); *Hoffer*, 128 F.4th at 440.

³⁵ *Jones v. Riot Hosp. Grp. LLC*, 95 F.4th 730, 735 (9th Cir. 2024).

³⁶ *Hoffer*, 128 F.4th at 440; *Jones*, 95 F.4th at 735.

³⁷ *Jones*, 95 F.4th at 735.

³⁸ *Gregory v. Montana*, 118 F.4th 1069, 1072 (9th Cir. 2024).

³⁹ *Nat'l Hockey League v. Metro. Hockey Club, Inc.*, 427 U.S. 639, 643 (1976).

⁴⁰ *Gregory*, 118 F.4th 1069.

⁴¹ *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

⁴² *Bistran*, 448 F. Supp. 3d 454.

⁴³ Fed. R. Civ. P. 26(b)(1).

⁴⁴ Fed. R. Civ. P. 26(b)(2)(B).

⁴⁵ Fed. R. Civ. P. 26(b)(3).

⁴⁶ Fed. R. Evid. 502(a).

⁴⁷ *Hearn v. Rhay* 68 F.R.D. 574, 581 (E.D. Wash. 1975)

⁴⁸ Fed. R. Civ. P. 37(e).

⁴⁹ *VOOM HD Holdings LLC v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33 (N.Y. App. Div. 1st Dep't 2012); *Pegasus Aviation I, Inc. v. Varig Logistica S.A.*, 26 N.Y.3d 543 (2015).

⁵⁰ *Brookshire Bros., Ltd. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014).

⁵¹ *Coleman v. Eddy Potash, Inc.*, 905 P.2d 185 (N.M. 1995), overruled on other grounds by *Delgado v. Phelps Dodge Chino, Inc.*, 34 P.3d 1148 (N.M. 2001).

⁵² *Smith v. Howard Johnson Co.*, 615 N.E.2d 1037 (Ohio 1993); *Elliott-Thomas v. Smith*, 110 N.E.3d 1231 (Ohio 2018).

⁵³ *Cedars-Sinai Med. Ctr. v. Superior Court*, 954 P.2d 511 (Cal. 1998); *Temple Cmty. Hosp. v. Superior Court*, 976 P.2d 223 (Cal. 1999).

⁵⁴ *Martino v. Wal-Mart Stores, Inc.*, 908 So. 2d 342 (Fla. 2005) (disapproving *Bondu v. Gurvich*, 473 So. 2d 1307 (Fla. Dist. Ct. App. 1984)).

⁵⁵ See *Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2d Cir. 2007).

⁵⁶ Tex. R. Civ. P. 196.4; *In re State Farm Lloyds*, 520 S.W.3d 595 (Tex. 2017).

⁵⁷ Cal. Civ. Proc. Code §§ 2031.010-2031.320 (West 2026); *id.* § 2031.060(c).

⁵⁸ Cal. Civ. Proc. Code § 2018.030(a) (West 2026).