



Applying the Legal Hold

Tips for Preserving Evidence in High-Stakes Litigation

With changes to the Federal Rules, the landmark *Zubulake*¹ and *Morgan Stanley*² cases, and the Supreme Court analyzing how document retention policies are enforced³, corporate practices around the retention/destruction of electronically stored information (ESI) have never been more important.

The “legal hold” operates at the intersection of litigation and corporate retention practices, and it has emerged as an almost-obligatory component of a company’s response to notice or reasonable anticipation of litigation.⁴ The basis of this obligation is the common law duty against spoliation; that is, the duty to avoid the loss of, destruction of, or failure to preserve information that may be relevant to pending or potential proceedings.⁵

In a pre-digital age, this duty was fairly straightforward: Don’t burn or shred the documents in your desk drawers or file cabinets. But modern businesses generate massive amounts of digital information, which is created and stored in an ever-expanding number of devices and locations, and which can be destroyed without any affirmative action. As a result, effective legal hold practices involve significantly more than merely issuing an internal letter and sitting back until the official discovery process begins.

Because the preservation of evidence is a crucial play in high-stakes litigation—involving many variables, exotic high-tech tools, and pitfalls for the unwary—consideration of the legal hold will be framed with the wisdom of Kenny Roger’s Gambler, who once said, “For a taste of your whiskey, I’ll give you some advice.”

“You got to know when to hold ‘em”

When is the duty to reasonably preserve evidence from loss or destruction triggered? When an entity “knew or reasonably should have known” that evidence may be relevant to pending or anticipated litigation. This fairly obviously includes receipt of formal notices, such as: a summons, complaint, or notice of investigation; a request for production or preservation letter; a court- or agency-issued preservation order or subpoena. The duty to preserve would also be triggered by events that indicate high potential for litigation—accidents, catastrophes, extraordinary stock-market events—but generally not simple posturing statements like: “I’m gonna sue you!”⁶

Of course, the contours of the “reasonably should know that evidence may be relevant to anticipated litigation” trigger are imprecise and context-dependent. For example, in *Lewy v. Remington Arms*, the court appeared

¹ See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y., May 13, 2003) (*Zubulake I*) and subsequent opinions. This employment discrimination case served as a platform for Judge Scheindlin’s detailed reasoning and explanation of modern discovery obligations. In various opinions throughout the case, Judge Scheindlin opined on the nature and scope of the duty against spoliation, the balancing test appropriate for reviewing the costs and benefits of discovery or cost-shifting arrangements, and the challenges and duties involved in the preservation and production of electronic evidence. UBS Warburg’s failure to preserve and properly produce electronically stored information formed the basis of an adverse inference order against defendant and the plaintiff was awarded a \$29.2 million verdict.

² See *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005). In this securities action, Morgan Stanley repeatedly failed to provide evidence in a timely fashion and improperly certified its productions as comprehensive and complete. Eventually, the trial court issued an adverse inference against Morgan Stanley based on spoliation of evidence resulting from failure to maintain email in readily accessible form and other evidentiary failings, which the court found “were done knowingly, deliberately, and in bad faith.” Coleman obtained a favorable verdict for \$1.4 billion, including approximately \$800 million in punitive damages assessed against Morgan Stanley. On appeal, the court, without raising the discovery abuses, reversed and remanded the case for entry of judgement in favor of Morgan Stanley. *Morgan Stanley v. Coleman (Parent) Holdings*, 2007 Fla. App. LEXIS 4167 (Fla. Ct. App., March 21, 2007).

³ *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005) (“Document retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.”) (internal citation omitted).

⁴ See *Zubulake IV*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (“Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ ...”)

⁵ “The policy underlying [the spoliation doctrine] is the need to preserve the integrity of the judicial process in order to retain [society’s] confidence that the process works to uncover the truth.” Indeed, the “destruction of evidence undermines two important goals of the judicial system—truth and fairness.” Lawrence B. Solum & Stephen J. Marzen, *Truth & Uncertainty: Legal Control of the Destruction of Evidence*, 36 Emory L.J. 1085, 1138 (1987) (quoted in *Rambus v. Infineon*, 222 F.R.D. 280, 288 (E.D. Va. 2004)).

⁶ See *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

to imply that frequent litigation surrounding certain products could give rise to a more expansive anticipation of litigation: in determining the legitimacy of retention policies “the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the *frequency* of such complaints, and the magnitude of the complaints.”⁷ The uncertainty around “reasonable” and “anticipation” can give rise to complicated questions: Are IP portfolio companies—who obtain patents primarily to exercise their legal rights against ongoing infringers—obligated to permanently retain purchase and strategy documentation because those materials are relevant to litigation, which is anticipated almost by virtue of the business model?⁸

Consequently, companies should consult counsel to establish triggering standards specific to the company’s circumstances and risk profile. In addition, companies should develop clear procedures for notifying appropriate legal personnel of actual or potential legal incidents, and should establish clear responsibilities for the quick investigation of the circumstances and potential “reason to anticipate” legal actions.

“Now ev’ry Gambler knows that the secret to survivin’ is knowin’ what to throw away and knowing what to keep.”

When litigation or investigation hits, lawyers are quickly tasked with determining *what* kinds of information are likely relevant to the issues, claims, and defenses involved, and with compiling a list of “key players” or custodians *who* are likely to possess the information. But, there’s a third dimension: *where*. In today’s digital business environment, most lawyers (and even many technologists) aren’t familiar with the wide range of forms and locations where such electronically stored information might exist.

Legal holds should function as an integrated component of a company’s overarching document retention policy: practically implementing the commitment to keep what must be kept, and benefiting from a carefully developed understanding of the volume, types, and locations of information generated, transacted, and disposed of by the company. Ideally, then, the company has invested attention and effort toward designing a modern document retention—or, more appropriate to the digital age, an information management—policy, which distinctly addresses electronically stored information and offers

Terminology

Litigation Hold. Legal Freeze. Litigation Freeze. Records Hold. Legal Preservation Order. The possible mix and match iterations for this concept are legion. “Legal” seems more apt than “Litigation,” as the obligation to preserve expands well beyond strict litigation situations to include internal or external investigations, responses to government or third-party subpoena powers, etc. In general, the key criterion is consistent use across the organization.

In detailing the effects of the legal hold, be conscious of the semantics of your instructions. Many attorneys will explain that the legal hold means “we must suspend our ordinary retention and destruction policy.” On its face, this can be true and well-intentioned, but it unduly focuses attention on destruction and implies that some change of course is necessary for corporate compliance. Consider whether it might sound better—to the ears of a jury or judge—to say: “Corporate policy clearly prohibits the destruction of information potentially relevant to legal actions affecting the company. This legal hold notice is issued, as prescribed in Paragraph X of our Corporate Retention Policy, to remind you of your ongoing responsibility to preserve certain information.”

⁷ 836 F.2d 1104, 1112 (8th Cir. 1988) (emphasis added)

⁸ Cf. *Rambus v. Infineon*, 222 F.R.D. 101 (E.D. Va. 2004) (involving the implementation of a document retention plan allegedly designed to eliminate potential evidence prior to patent suits).

detailed descriptions of the “wheres” of digital data. However, if the company’s document retention policy is archaic or its cognizance of its own data systems isn’t particularly robust, then the attorneys involved with the legal hold process must quickly familiarize themselves with the critical components of their client-company’s information technology.

An understanding of IT terms like “metadata” and “native files” and “scrubbing” is a modern necessity, but it’s hardly sufficient to meet the demands of litigation and investigation. In the wake of *Zubulake* and *Morgan Stanley*, it’s increasingly clear that courts (and opportunistic opposing counsel) will demand a fairly high degree of IT savvy from attorneys involved in the discovery of ESI. Attorneys must have a functional familiarity with their client-company’s IT infrastructure in order to:

- understand how an effective legal hold can be developed and implemented across multiple data systems (e.g., email, file servers, employee workstations);
- understand the processes and difficulties of collecting data across these multiple data systems;
- identify critical data stewards who should receive internal preservation letters and who might assist with technological solutions for preservation;
- strategize about implementing the hold, managing multiple holds, supervising compliance, and notifying personnel when holds expire;
- be prepared to discuss the relative “accessibility”⁹ of certain information in discovery negotiations; and
- most crucially, be informed and aware when making representations and certifications to the court.

The onus put on counsel by the *Zubulake* opinions is substantial—but certainly not beyond the capacity and savvy of most accredited attorneys.¹⁰ Too often, however, corporate counsel’s internal understanding of the company’s data-management systems is developed on the fly, *after* a notice of litigation triggers the duty to preserve, and while the legal hold is being developed and the countdown toward systematic auto-deletion ticks away. This leads to hastily assembled ad hoc¹¹ solutions, costly over-investments of time and workforce, and general uncertainty about the effectiveness of the legal hold and litigation response efforts.¹² Prudent counsel should, therefore, familiarize themselves with their client-company’s IT department and key contacts in advance of major legal events, so that an organized and already-understood process can unfold as a matter of course.

⁹ An “accessible vs. inaccessible” dichotomy is the present framework for evaluating the burden of discovery collection and the justification for shifting the costs of production from the respondent to the requesting party. See *Zubulake I*, 217 F.R.D. 309 (S.D.N.Y. 2003) (discussing accessibility and cost-shifting); *Zubulake IV*, 220 F.R.D. 212, 218; *Zubulake V*, 229 F.R.D. 422, 425-26 (S.D.N.Y. 2004) and the amendments to Federal Rule of Civil Procedure 26(b)(2)(B).

¹⁰ To implement a legal hold, “counsel must become fully familiar with her client’s document retention policies, as well as the client’s data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm’s recycling policy. It will also involve communicating with the “key players” in the litigation, in order to understand how they stored information. In this case, for example, some UBS employees created separate computer files pertaining to *Zubulake*, while others printed out relevant emails and retained them in hard copy only. Unless counsel interviews each employee, it is impossible to determine whether all potential sources of information have been inspected.” *Zubulake V*, 229 F.R.D. 422 (S.D.N.Y. 2004).

¹¹ Such as situations, as in *Zubulake*, where “some UBS employees created separate computer files pertaining to *Zubulake*, while others printed out relevant emails and retained them in hard copy only.” *Zubulake V* at 432. Successful legal hold efforts begin with understanding the systems and capabilities already in place, so that clear instructions for consistent preservation methodologies can be issued and idiosyncratic deviations from standard practice can be identified and accounted for.

¹² See, e.g., *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 Extra LEXIS 94 (Fla. Cir. Ct., Mar. 23, 2005).

Once the legal action is sufficiently clear that the players involved can be identified, counsel should confer with these specific personnel in order to understand their actual document retention and preservation practices. The formal language of the company's document retention policy and the structural environment created by the company's IT architectures are important, but defensible preservation requires working directly with potential custodians to account for idiosyncratic document management habits.¹³

Data Map

A particularly useful opportunity for collaboration between the legal and IT departments is the development of a "data map" that profiles, at varying degrees of "resolution" (and at varying levels of time and money investment), the company's sources and locations of ESI (or, most ambitiously, corporate information generally). The objective of the data map is to have an up-to-date resource that sets out salient details of the company's different active data creation and storage systems, including:

- email, including information about the email applications, server organization and physical locations, and backup protocols;
- instant messaging, voicemail, and Voice Over Internet Protocol applications, which may make persistent records of electronic communications;
- network storage and file servers, including information about server organization, physical location, and backup protocols;
- a list of applications and file types in use at the company, including details on proprietary or unique applications and integrated databases (from which information can't easily be separated as "a file");
- workstation distributions and configurations;
- remote user set-up (i.e., are employees able to VPN in from their home computers?); and
- distribution and use of mobile devices, including laptops and PDAs, with specific attention to whether data on these devices is captured or "synched" in any formal fashion.

¹³ See *Zubulake V* at 432.

Managing Multiple Holds

Issuing, implementing, and supervising even one legal hold is a technical challenge; keeping track of multiple, often overlapping and "similar, but different" holds adds another order of magnitude to the complexity and stakes. Tracking tools range from the simple and ad hoc, such as spreadsheets compiled and maintained by the legal department, to the market-driven and professionally developed. Software solutions enable counsel to track each legal hold from issuance and acknowledgement through collection, processing, and eventual rescission of the hold order—and can automate the process of providing status and reminder notices to appropriate custodians. These databases will indicate where multiple holds overlap, so that there is less chance of confusion and spoliation when one hold is lifted while an overlapping one remains effective. Perhaps most importantly, these process-solutions demonstrate the company's good-faith efforts to meet its anti-spoliation duties across the entire range of active obligations.

Similarly, where companies face the likelihood of substantial numbers of follow-on litigations, it may be prudent to consider the "archiving" of the materials gathered under these similar legal holds or discovery efforts. Some e-discovery providers offer litigation repositories, into which potentially relevant information can be deposited and accessed, so that reviews for responsiveness and privilege can be done one time and these evidence-profiling conclusions preserved for later use.

These automated tools may involve greater investment than a homemade spreadsheet, but for companies frequently involved in litigation, or facing the possibility of multiple follow-on actions, it's difficult to overestimate the savings in time, reductions in complication and risk, and gains in confidence and administrative ease that can be realized by implementing appropriate and useful professional solutions.

The data map might also include details on the names and roles of key data “stewards”: IT and records management types who may not be “custodians” or key players in the litigation, but who manage and control the technologies of document creation and destruction. These personnel will be important in the legal hold process, as they are the folks capable of “flipping the switches” to prevent data destruction or set-up internal preservation and collection tools.

The data map will serve as both a reference resource—enabling counsel to understand “who has what kind of information where”—and also as a framework for actual collection efforts and general documentation. With the various information silos identified and the key players added, the map can be converted to a checklist and collection log, allowing counsel to track and document progress as the formal legal hold is translated into actual preservation and collection practices.

Some Cards to Have Up The Sleeve

Developing and maintaining template materials and a “legal hold toolkit” is like stashing quality cards up your sleeve (or, if you find the cheatin’ analogy dishonorable, consider these tools to be your hole-cards). This toolkit might include a range of materials designed to minimize the cost and chaos of addressing critical discovery process matters when litigation or investigation ensues, such as:

- the company’s current document retention policy;
- any available data maps;
- data collection checklists;
- pre-fabricated strategy guidance;
- template letters (see below)

In addition, the toolkit might identify something like a “Litigation Response Team”—some (loosely) organized “committee” composed of legal, IT, records management, and risk management personnel who are collectively familiar with the importance and process of anti-spoilation preservation. This tool might be as minimal as a list of key contacts in the company’s IT and records management departments—just some preliminary guidance so that an attorney tasked with issuing and supervising the legal hold can quickly convene the personnel necessary to implement available technological preservation solutions.

Consider developing template letters that permit the quick-and-easy combination of general, up-to-date boilerplate language with case-specific details appropriate to a variety of uses:

(1) Internal preservation letter

The internal preservation letter should be issued to both key custodians (“key players” with knowledge or potential evidence substantively relevant to the litigation) and key stewards (personnel responsible for setting up and maintaining the IT and records systems in which custodians’ data exists), in order to establish two lines of anti-spoilation defense. Custodians will be aware that they are not to destroy pertinent information, and stewards will be aware that certain custodians’ data should be preserved at the infrastructure level (e.g., not auto-deleted when the emails reach a certain age).

Boilerplate sections should include:

- recitation of the corporate commitment to preservation of evidence and reasonable cooperation with judicial/governmental requests;
- references to the current version of the corporate retention policy (and refresher instructions on how employees should access and review the policy);
- contact information for designated authorities handling the matter, at departmental levels if appropriate;
- a simple statement acknowledging the complexity of preserving evidence in today's digital business environment, paired with the recognition that business must go on—but then followed up by a reiteration of the point that all reasonable efforts will be made to identify and preserve potential evidence;
- a detailed and expressly non-exclusive list of potential media-types or “locations” in which potential evidence might exist.

Situation-specific sections should:

- present a high-level explanation of the immediate matter;
- detail the criteria for identifying potentially relevant evidence; and
- detail the procedure for preservation of information deemed potentially relevant; i.e., who and how to notify; whether the information should be preserved in place or delivered (via forensically sound methods!) to a central repository.

The internal preservation letter should contain some return receipt through which custodians and stewards can acknowledge that they received, reviewed, and fully intend to comply with the preservation guidance.

(2) External preservation letter

The external preservation letter boilerplate would be a detailed (but non-exhaustive, always) itemization of the document and ESI types that your client-company believes must be preserved by the other

Ongoing Duty to Supervise the Hold

The internal preservation letter that implements the legal hold is not a sufficient and defensible effort toward preservation. Judge Scheindlin, in *Zubulake V*, noted that “[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.”

Consequently, counsel should take calculated steps to ensure that the hold is being complied with. For example, counsel should regularly issue reminders and status updates to the key players and data stewards, to prevent their diligence from becoming stale and relaxed. Furthermore, a compilation of legal hold letters and follow-on notices can be used to inform any new employees who have joined the organization in a capacity that obligates them to comply with a pre-existing hold.

Given the important role of technology in the preservation efforts, counsel should regularly consult with the data stewards to ensure that the tools implemented for preservation and collection efforts are operating as planned.

Judge Scheindlin was appropriately realistic, however, and her opinion reminds us that the overall touchstone for most discovery matters is reasonableness, certainly where the relationship between outside counsel and clients is at issue: “Above all, the requirement must be reasonable. A lawyer cannot be obliged to monitor her client like a parent watching a child. At some point, the client must bear responsibility for a failure to preserve.” The reasonableness standard may require demonstration, however, and therefore Judge Scheindlin recommends that counsel and the company carefully document the issues faced, the decision-making processes, and the concrete actions taken throughout the implementation, preservation, and collection stages.

party. The proper balance between specificity and generality is difficult: Greater specificity establishes notice, but compiling many specific demands effectively becomes a comprehensive request for “anything and everything,” which may trigger backlash or symmetrically excessive demands from the other party. The amendments to the Federal Rules of Civil Procedure impose new requirements for the negotiation of ESI discovery issues, and the multiple instructions to discuss these issues “early and often” suggest that the courts are hoping for cooperative efforts in narrowing the scope and burden of discovery.

(3) “Rebuttal” to external preservation request

This letter is designed to muster current case law and best practices “dicta” toward responding to incoming preservation requests that are often—by design—extremely vague, overbroad, and impossibly cumbersome. The letter should collegially:

- express the company’s clear intent to comply with the reasonable duty of preservation;
- provide a synopsis of case law and materials that unpack the “reasonableness” of preservation efforts,¹⁴ the legitimacy of document destruction,¹⁵ and the FRCP safe-harbor provision;¹⁶
- detail the complexities of the company’s IT architecture and the potential costs associated with preservation/collection (in order to lay cost-shifting groundwork early); and
- request assistance from the requesting party in narrowing down the focus and cost of preservation efforts.

If there’s any “ace advice” to be squeezed from our discussion of the high-stakes game of discovery in the digital age, it’s this: Develop your legal hold strategies and structures before the discovery-dealin’ unfolds. By doing so, you improve your odds and reduce the gamblin’ involved—because you already know about the cards you’ll be playing. In a very liberal (and I hope not inexcusable) rephrasing of the Gambler’s wisdom:

You never count your [corporate information] when you’re sittin’ at the table; the smart time for countin’ is before the dealin’s done.

¹⁴ See, e.g., *Zubulake IV*, 220 F.R.D. at 217 (“Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly ‘no.’ Such a rule would cripple large corporations ... that are almost always involved in litigation.”)

¹⁵ *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005)

¹⁶ Amendment to Federal Rule of Civil Procedure Rule 37(f).

The Discovery Experts: *Strategic Records and Information Management Group*

LexisNexis Discovery Services has the right consulting and technology choice for every discovery need. Top law firms, corporations and government agencies rely on the LexisNexis® products and services, Applied Discovery®, Concordance™, and Hosted FYI™, to meet their discovery obligations on time, accurately and cost-effectively. Services include data collection, forensics, media restoration, data filtering, data processing, online review and document production in the format that each matter requires. The *Strategic Records and Information Management Group* uses its rare blend of legal and technical expertise to help corporate clients fulfill discovery requests calmly and with confidence.

For more information or to contact the experts, please visit lexisnexis.com/discovery.

