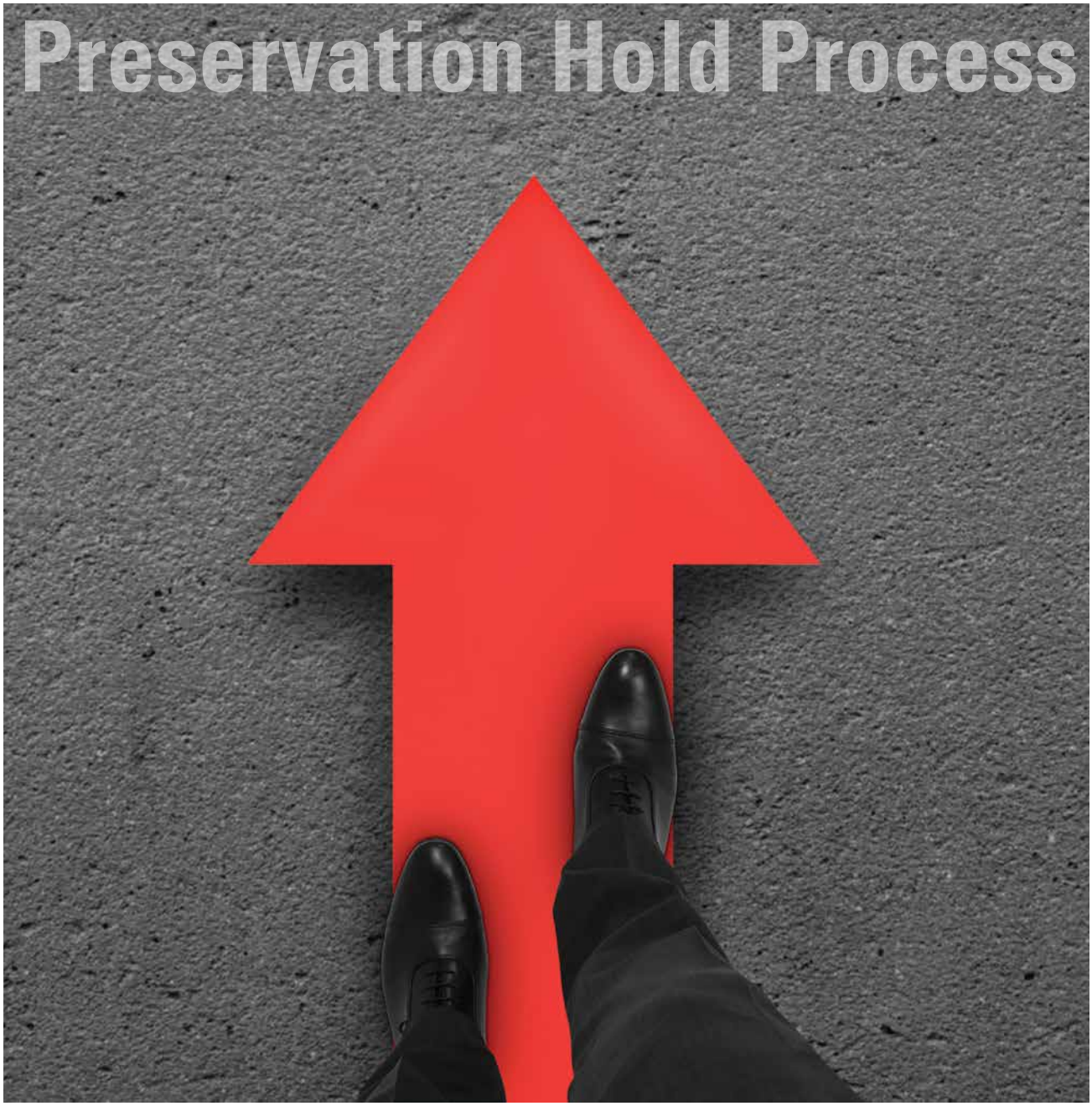
Critical Steps to Creating a Consistent Preservation Hold Process



Richard Vestuto, J.D., and Bill Piwonka

Many organizations struggle to develop a cost-effective and defensible hold process. This article provides six steps to help organizations plan, automate, and communicate a legal hold process that will improve efficiency, reduce risks, and meet their preservation obligations.

Any organization subject to large, complex, high-stakes lawsuits or investigations requires a repeatable process for preserving potentially relevant electronically stored information (ESI). Yet for many organizations, the preservation process is often chaotic, time-consuming, and error-prone. This is often because they rely on disparate technologies or manual processes to support preservation efforts, with potential mistakes occurring due to poor coordination and sloppy hand-offs. These errors are frequently amplified by the many complexities and challenges that can complicate preservation efforts.

One such challenge is dealing with employee status changes. Employees go on leave, move to new positions or different business units, or depart the organization altogether. While employee movement is a routine element of modern business life, it takes on critical significance in the context of e-discovery, where failing to properly track employees can result in data spoliation and severe sanctions.

Having a legal hold process that preserves data throughout the e-discovery life cycle – from initiation to release and data deletion – is critical. This article walks through several critical steps for creating a consistent preservation hold process.

Step 1: Understand the Legal Hold Life Cycle

At its most basic level, a legal hold is a form of notification, often an e-mail, informing the recipient that a lawsuit has been commenced or is reasonably anticipated and that the party receiving the e-mail must preserve all data potentially related to the subject matter of the case.

While the basic process of issuing, monitoring, and documenting legal holds is fairly similar across many organizations, priorities for preserving ESI vary depending on the organization's size, type, and industry. Large organizations typically have hundreds or thousands of employees that are dispersed geographically and spread among a number of business units. The legal team needs to be able to create, acknowledge, and track legal holds efficiently. Simply sending out a legal hold notification e-mail does not equate to a defensible process.

Basic Steps

Following are basic steps organizations should consider to help ensure a defensible preservation process:

1. Confer with key stakeholders, including information technology (IT) and human resources (HR), to confirm that every person related or potentially related to the legal matter understands the scope of the preservation obligations.
2. Suspend any automatic deletion or purging of e-mail and other key information systems by taking these actions:
   a. Pull current backup tapes from rotation or recycling to ensure data is preserved without risk of spoliation.
   b. Identify any laptop/desktop backup routines running on a scheduled basis and archive the most recent backups.
   c. Stop recycling or reissuing hardware.
   d. Stop purging user accounts and individual network shares for departed employees.
3. Issue legal hold notices when litigation is reasonably foreseeable, which is usually before notice of suit is given.
   a. Write the notice in "plain English," describing the nature of the matter and the issues at hand.
   b. Give clear instructions to employees not to modify, destroy, delete, or hide any electronic or hard copy data related to the commenced or anticipated litigation or investigation, including all paper or ESI, other data stored on the company's computer systems and storage media, or any other electronic data.
   c. Take steps as early as possible to preserve data from user-assigned laptop/desktop computers and mobile devices.
4. Interview the key players subject to the legal hold to confirm they understand their legal obligations as well as to get their help identifying other employees or data that may be subject to the preservation obligation.
5. Remind employees of their preservation obligations on a regular schedule to facilitate compliance.

Issue legal hold notices when litigation is reasonably foreseeable, which is usually before notice of suit is given.

6. Release the hold as soon as the underlying matter is resolved. This allows the electronic evidence to be deleted according to the company's regular retention policies, assuming it's not subject to preservation obligations on another matter.

Key Stakeholders

Legal holds occur at the very crossroads of an organization's people, processes, and technologies. They also intersect with business units across the organization, including legal, IT,

records management, HR, and compliance, among others. As with any business-critical practice, it is important that basic legal hold requirements are communicated to each business unit and that each knows its specific role in the process.

It's also important to establish a steering committee comprising these stakeholders to help ensure the organization's preservation protocols are applied consistently on every matter, while not disrupting other business processes. This will help arm counsel with the critical details needed for effective case negotiations, including the backup system status, relevant search terms, date ranges, and other qualifiers that can narrow the scope of discovery. It will also empower IT and records management to facilitate the defensible deletion of ESI when it no longer has business or legal utility. The committee should be chaired by a C-level executive to help ensure recommendations are incorporated into policy.

… it is important that basic legal hold requirements are communicated to each business unit and that each knows its specific role in the process.

Step 2: Avoid Common Preservation Mistakes

Many legal hold mistakes can be traced back to the common causes described below.

Poor Custodian Identification and Tracking

This includes failing to diligently identify all likely custodians when litigation becomes reasonably expected and not conducting effective custodian interviews to learn more about the case or other potential custodians.

Poor Data Source Identification

If an organization doesn't know where the data resides or who has access to that data, it will most likely fail to properly preserve it. Data residing on file shares, detachable drives, and third-party systems can often be overlooked. Don't forget to examine these common enterprise data sources that are often subject to discovery:

- Employer-Controlled Sources
  - E-mail servers (mailboxes of individual e-mail users)
  - File servers and print servers (including individually assigned network stores or "home shares")
  - Network drives ("group shares" accessed by multiple individual users)
  - Archival data on backup tape or other storage media
  - E-mail journaling systems
  - Document management systems
  - Proprietary structured databases (e.g., databases containing HR, customer, or sales data)
  - File shares and other web-based collaboration sites
  - Social networking sites and services/accounts used and maintained by the company
  - Video and audio systems (e.g., voicemail)
  - Legacy data (e.g., ESI generated by computer programs no longer used by the company)
  - Hard copy document archives maintained by the company (including offsite storage)
  - ESI maintained in hosted databases in connection with prior litigations / investigations
- Employee-Controlled Sources
  - ESI found on user-assigned laptop/desktop hard drives, including word processing, spreadsheets, images, and other text-based files
  - Locally stored e-mail archives (user-archived PSTs, OSTs)
  - Individual backup and temp files
  - Internet usage data (e.g., cookies)
  - Portable storage media (e.g., user-controlled external hard drives, flash drives, CD/DVDs)
  - Company-issued mobile devices (e.g., cell phones, tablets)
  - Hard copy documents maintained by the employee
  - Cloud-based storage
  - Social media and personal e-mail accounts

Poor Hold Discipline

Examples of this are issuing legal holds verbally, sending a written hold notice without any follow-up notices, and not escalating to a custodian's superior when the custodian is non-compliant.

Poor Communication

Issuing a legal hold without enough details to the custodian or stakeholders, for example, can result in custodian non-compliance or omission of potentially relevant ESI.

Lack of Protocols

Established protocols are critical to ensuring data sources are protected and for preventing ad hoc approaches for identifying ESI, search criteria, online and offline repositories, and employee status changes.

Step 3. Understand Legal Ramifications of Failure

A lack of planning, an over-reliance on manual, error-prone methods, and poor communication between

IS INFORMATION YOUR ALLY OR YOUR ENEMY?

NEXT LEVEL™
information governance assessment

Your business data is doubling by the year. And all this new data can either help you or hurt you. Find out what it's doing for your company with the Next Level Information Governance Assessment. You'll discover areas of strength and opportunities for improvement. In the end, you will be empowered to increase organizational transparency and data integrity while decreasing risk.

Start turning information into an asset by visiting **arma.org/nextlevel**.

various stakeholders involved in the preservation process can lead to severe sanctions; courts have made it very clear that ignoring the problem no longer works. The two recent case law examples below reinforce the importance of having solid preservation practices.

Failure to Preserve Employee Data

A leading IT services company was embroiled in a discrimination claim with the U.S. Equal Employment Opportunity Commission (EEOC). The company terminated an employee who had filed a claim in November of 2009, and he filed a second EEOC charge in December of 2009, claiming he was terminated in retaliation for his discrimination claim.

Automation can help prevent the legal and IT teams from making preservation mistakes, as well as save time, promote consistency, and improve communication.

The terminated employee had worked remotely, and all or nearly all of his data was located on his work laptop, which he returned to the company upon termination in December. The company subsequently wiped the laptop and reissued it to another employee the following month.

A couple of years later, the terminated employee filed a discrimination suit against the company under 42 U.S.C. § 1981 and state civil rights laws. The company did not issue a legal hold until three months later. Additionally, a year later, the employee's former supervisor also left the company, and he later testified that he did not back up any of his own data before returning his laptop. Apparently, the data was lost.

The company claimed that the data sought by the employee was not stored centrally at the company; later that assertion was contradicted by testimony by company witnesses. The employee alleged that the company deleted responsive data on both his laptop and his supervisor's laptop and moved for sanctions.

The court found that the company was grossly negligent in its duty to preserve and granted an adverse inference instruction with respect to the data stored on the laptops. The terminated employee's request for sanctions was granted in part and denied in part. The company was not sanctioned for the destruction of data on the employee's computer, but the court issued an adverse inference instruction for the spoliation of the data on the supervisor's hard drive.

Failure to Interview Custodians

In a litigation involving two drug manufacturing companies, in two separate opinions, the court addressed the obligations with regard to the preservation and collection of data and the obligation of counsel to obtain input from relevant custodians.

In the first opinion, the court ordered an extensive forensic examination of the plaintiff's data by a neutral third party and crafted a protocol for production of the data identified by the applied search terms.

In the second opinion, the court confirmed a basic rule that counsel must carefully craft the appropriate keywords, with input from the custodians, as to the words and abbreviations they use. The court ordered counsel to obtain search word input from all custodians and to pay a portion of the attorney's fees awarded.

Step 4: Eliminate Manual Processes

Automation is one area where technology becomes indispensable to a defensible, efficient preservation process. Preservation requirements tend to change over time. For example, as more custodians are added to a legal hold, the complexity and the effort required to manually track the process increases exponentially. A single custodian may interact with five or six data sources.

Automation can help prevent the legal and IT teams from making preservation mistakes, as well as save time, promote consistency, and improve communication. Areas of the preservation process that can be automated include:

Creating Legal Hold Notices

Users should be able to automate the legal hold process by leveraging customized templates that are created based on case type or legal objective and can be reused on similar matters.

Automating Custodian Interviews

Surveys can help custodians better understand their preservation obligations, as well as help the legal team learn more about the matter and its potential scope. Having the system automatically send out the interviews may eliminate the need to recreate interviews for every new matter and allow responses to be added to the system of record automatically.

Tagging Notices

Tags, or identifiers that attach to a preservation notice, such as a brief description of a matter or the matter name, can be automatically attached to all relevant preservation notices to eliminate tedious, repetitive, and error-prone information entry and inform both IT and legal across matters to avoid repeat of work.

Establishing Workflows

Establishing automated workflows

can ensure approvals are received at specified steps in the preservation process before moving forward. They can also ensure copies of holds and interviews are automatically issued to designated recipients. For example, organizations should be able to set up an automatic process to ensure that an attorney approves a hold notice before it's issued and approves the interview before it goes out.

Sending Reminders, Escalation Notices

It's important to keep in mind that recipients of legal holds have day-to-day business responsibilities and will likely need to be reminded of their hold obligations from time to time. The preservation system should allow the legal team to automate such notices on a predetermined schedule, as well as escalate them to supervisors to help ensure that non-responsive custodians take a requested action.

Step 5: Track Employee Changes

When an employee departs an organization, it is common practice for IT to delete, reimage, or destroy the individual's data from local devices, as well as shared servers, and reissue the equipment to someone else. What often gets overlooked in the process is that the departed employee may have been subject to a preservation obligation, which persists regardless of whether the person is actively employed at the organization.

While departing employees may present the greatest risk for inadvertent data spoliation, it's important to recognize that other employee status changes, such as extended leaves of absence, departmental transfers, relocations, promotions, or even last name changes can also warrant corrective action.

It's important to track all employee movement to prevent data spoliation. Technology is advancing to automate this process. By integrating the organization's HR and e-discovery systems, the legal team can eliminate the manual, time-consuming review of daily spreadsheets issued by HR and automatically be alerted of employee changes requiring corrective action, as can IT and other impacted business units.

For example, if an active custodian is changing departments, legal may respond by simply updating its records to reflect the change and send a reminder e-mail to the employee so he or she knows that the terms of the legal hold still apply.

Or, if an employee is leaving for maternity/paternity leave, IT needs to be notified to ensure that the systems and data won't be compromised as a result of the prolonged absence. This type of information can also help legal and IT understand why data volumes vary greatly during discovery – potentially explaining away suspicions of missing data or spoliation.

Step 6: Be Proactive and Educate

One of the easiest countermeasures to data spoliation is awareness and education. It's critical that legal teams educate their counterparts in HR and IT, as well as other employees, that preservation obligations persist.

In some work environments, it works well to have a single member of each team participate in regular, in-person meetings, which help promote a more active, engaged dialogue around the key issues. Ultimately, the goal is to come up with a plan that strikes a balance between the organization's legal obligations and its desire to minimize operational expenses. To get started in developing this plan, it's important to take the following steps.

Understand the Data Landscape

Gain a level of familiarity and comfort with the organization's data landscape, including an understanding of the nature and location of key data sources, a strong working relationship with important IT contacts who can assist in getting to relevant ESI, and a general sense of the significant data risks and issues that may arise as a result of the format or location of certain ESI.

Talk to Custodians

The duty to preserve potentially relevant ESI applies to all custodians, including those who may have had only a passing encounter with the central issues in the litigation. Custodians not only have the relevant data, they also have information that can be extremely valuable in tracking down other responsive ESI and developing a case strategy. To be effective, the custodian interview process should be conducted in a consistent, repeatable manner to help ensure that the resulting information can be easily processed and acted upon.

…keep in mind that recipients of legal holds have day-to-day business responsibilities and will likely need to be reminded of their hold obligations from time to time.

Document the Process

Make it a priority to document the preservation process. Having a documented process fosters a culture of communication and efficiency because team members know exactly what's expected of them and under-

stand their tasks in the context of larger objectives. In the event that e-discovery mistakes do occur, a well-documented process can also mitigate repercussions by demonstrating that the mistakes were likely not systemic in nature, but rather were simple, isolated oversights.

Result: A Cost-Effective, Defensible Process

Preservation obligations are generally well understood by corporate legal teams. Where many organizations struggle is in developing preservation processes that help ensure these obligations can be sufficiently met in a defensible, cost-effective fashion. Many legal hold mistakes can be traced back to a lack of planning, an over reliance on manual, error-prone methods, and poor communication between various stakeholders involved in the process. By following the steps listed above, organizations can effectively modernize their preservation processes, thereby reducing risk and improving efficiency.

Note: *This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. Deloitte does not provide legal services and will not provide any legal advice or address any questions of law.* **END**

Richard Vestuto, J.D., can be contacted at rvestuto@deloitte.com. *Bill Piwonka can be contacted at* bill.piwonka@exterro.com. *See their bios on page 47.*