Reducing the Cost and Headache of e-Discovery with a Comprehensive Retention Plan for Electronically Stored Information

By

Fernando A. Bohorquez
Alberto Rodriguez
# Table of Contents

I. INTRODUCTION ............................................................................................................. 3

II. THE BENEFITS OF A ROBUST ESI RETENTION POLICY ........................................... 4
   A. A Comprehensive ESI Plan Significantly Reduces e-Discovery Litigation Costs .......................................................... 4
   B. A Well-Prepared ESI Retention Plan Can Reduce the Burdens on In-House Counsel ................................................................. 10

III. HALLMARKS OF AN EFFECTIVE ESI RETENTION POLICY .................................... 12
   A. An ESI Retention Policy Should be Reasonable ............................................ 13
   B. An ESI Retention Plan Should be Tailored To The Company ...................... 14
   C. Developing a Clear ESI Retention and Destruction Schedule .................... 16
   D. Consistent Enforcement and Implementation of ESI Plan ............................ 19

IV. CURRENT E-DISCOVERY BEST PRACTICES AND SOFTWARE SOLUTIONS ......................... 20
   A. Identification ........................................................................................................ 20
   B. Legal Hold .......................................................................................................... 20
   C. Collection ........................................................................................................... 21
   D. Scalability of Solutions ...................................................................................... 21

V. CONCLUSION ................................................................................................................ 22
I. INTRODUCTION

Maintaining a well-developed retention and destruction policy for electronically stored information (ESI) has never been more important than it is today, as companies of all sizes confront a growing and never-ending stream of electronic data. This constant flow of ESI ranges from mundane business operations to trade secrets, financial data, and statistical analyses. With such large quantities of ESI, it is tempting for some businesses to simply take the path of least resistance and retain all ESI for as long as possible. Other companies take the opposite approach and delete their ESI as soon as it loses its operational value. Still others have actually developed an ESI plan but fail to take the necessary steps to implement it properly. All of these scenarios may lead to disastrous consequences should litigation arise and a company has either stored too much ESI in outdated formats or fails to retain it to meet legal obligations.

Companies that plan and implement an effective ESI retention plan can reap many benefits, including: (1) facilitating easier and more timely identification of, and access to, necessary information; (2) controlling the creation and growth of information; (3) reducing operating and storage costs; (4) meeting statutory and regulatory retention obligations; and (5) meeting discovery obligations that arise before and during litigation.¹ A well-organized ESI plan accounts for the creation, maintenance, storage, and, when appropriate, destruction of a business’s ESI. Such a plan gives company management a bird’s-eye view of the flow of electronic information and helps to identify potentially reams of information that have no value to the company and may pose substantial legal and regulatory risks. A robust ESI retention policy will purge unnecessary information from a business organization’s system, thus freeing the business from having to backtrack and review tons of irrelevant information once litigation

---

arises. An ESI plan can also be useful in simply identifying ESI needed to meet legal and regulatory obligations expeditiously. While establishing an ESI retention plan will initially require an investment on the part of the company, that investment will pay off in the form of a more efficient flow of information and through reduction of litigation-related costs.

II. THE BENEFITS OF A ROBUST ESI RETENTION POLICY

A. A Comprehensive ESI Plan Significantly Reduces e-Discovery Litigation Costs

There is a significant economic advantage to having a solid ESI retention policy in place as a business organization advances through the e-discovery process. The Electronic Discovery Reference Model (EDRM) divides e-discovery into nine “iterative” and “non-linear” phases as shown in the chart below.² An ESI plan may provide cost savings in at least the first six phases of e-discovery as demonstrated by the EDRM, including (1) information management; (2) identification; (3) preservation; (4) collection; (5) processing; and (6) review. The following EDRM chart³ illustrates the stages a typical e-discovery process may take:

---

³ Id.
An ESI retention plan greatly helps with information management by essentially providing a starting point for the initiation of document retention and destruction policies for each category of ESI. A robust and consistently applied ESI retention plan can ensure that when documents are deleted, their destruction is done pursuant to a document retention policy that is defensible against claims of spoliation – or the intentional destruction, alteration or concealment of evidence. Importantly, Rule 37(e) of the Federal Rules of Civil Procedure (Federal Rules) maintains a safe harbor for a party’s failure to produce ESI when it is lost as the result of good faith compliance with a company’s document destruction policy. Rule 37(e) provides, in part, that “a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” The routine destruction of documents is therefore legal and completely appropriate as long as it is done pursuant to an ESI retention policy applied in good faith.

---

4 Black’s Law Dictionary 1531 (9th ed. 2009); Sedona Guidelines, supra note 1, at 25.
When ESI such as e-mails are deleted as part of an established ESI system and document management policy, courts have routinely found that the deletion was made in good faith and falls within Rule 37(e)’s safe harbor. For example, in *Kermode v. Univ. of Mississippi Medical Center*, plaintiff alleged that defendants failed to preserve certain e-mails that he had requested during the discovery process and sought a sanction in the form of a default judgment.⁶ The court found that the plaintiff had not shown that there were, in fact, relevant e-mails other than those produced by defendants. The court also determined that even if relevant e-mails existed, they would have been purged pursuant to a routine data destruction policy. Finding that there was no other evidence of bad faith, no sanctions were warranted.⁷ Similarly, in *Southeastern Mechanical Services, Inc. v. Brody*, the court found that no spoliation sanction was appropriate because the automatic overwriting of back-up tapes containing a key custodian’s e-mails was part of the company’s routine document management policy and no other evidence of bad faith was offered.⁸ A company may therefore point to the existence of a document destruction policy to demonstrate that it would not have access to documents prior to a certain date, thus alleviating it burden to produce such documents.

An ESI retention plan also greatly facilitates the ESI identification process. Because an ESI plan tracks very disparate pieces of ESI – from hard drives to remote servers – large repositories of ESI should all be accounted for and more easily found. A clear example of the need to effectively and quickly identify ESI at the very early stages of litigation can be found in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*⁹ The *Coleman* case is a

---

⁷ Id. at *6.
cautionary tale of the need to know where ESI is maintained – especially the ever-challenging back-up tapes.

In *Coleman*, the plaintiff brought a motion for discovery sanctions due to defendant Morgan Stanley’s alleged destruction of e-mails and non-compliance with the court’s discovery orders. In June 2004, Morgan Stanley provided the plaintiff with a written certification that it had complied with its disclosure obligations. However, shortly before providing the written certification, Morgan Stanley had become aware that more than 1,400 back-up tapes had been found at its facility in Brooklyn, New York. Amazingly, 1423 back-up tapes (the Brooklyn Tapes) had not been processed by Morgan Stanley’s outside vendor and had thus not been searched prior to Morgan Stanley’s discovery certification. The Brooklyn Tapes contained e-mails dating back at least to the late 90s. In addition, Morgan Stanley failed to timely produce e-mails from several other batches of back-up tapes, including a group of 738 8-millimeter back-up tapes found in Morgan Stanley’s facility in Manhattan in 2002, 169 back-up tapes found in January of 2005 that were allegedly misplaced by Morgan Stanley’s New Jersey storage vendor and 200 back-up tapes discovered in locations known for storage of back-up tapes. These tapes had also not been processed by Morgan Stanley’s outside vendor. In total, Morgan Stanley failed to locate and search over 2,200 back-up tapes necessary to timely comply with its disclosure obligations. The court found that Morgan Stanley committed various willful discovery violations such as the deletion of e-mails and late production of relevant information. The court allowed the plaintiff to give the jury an adverse inference instruction permitting the

---

10 *Id.* at *1.
11 *Id.* at *2.
12 *Id.* at *4.
jury to infer that the missing ESI was evidence of Morgan Stanley’s fraudulent conduct.\textsuperscript{14} The jury subsequently returned a $1.4 billion\textsuperscript{15} verdict in favor of the plaintiff.

An effective ESI retention policy also aids the preservation and collection phases of the e-discovery process by outlining procedures for a litigation hold – a directive within a business organization advising employees of their duty to preserve and maintain documents and other materials that may be relevant to a lawsuit or governmental investigation.\textsuperscript{16} This process is normally accomplished with an e-mail notification sent to individual custodians of electronic materials and instructs them not to destroy or alter any potentially relevant materials. Once a litigation hold has been issued, counsel may take steps to collect relevant information from individual custodians that fall under this directive.

An effective ESI plan is a significant method of reducing the cost impact of e-discovery with respect to data processing and review. An effective ESI plan, as discussed above, incorporates routine destruction of documents that no longer possess any business, legal or regulatory purpose. This purging process ultimately means fewer data sets that counsel will send out to a discovery vendor to process – or convert to a reviewable format – and review by attorneys. Processing costs vary depending on the type and quantity of data. However, there is one cost principle that remains constant – less data to process and review means less money spent on e-discovery. For example, a 100-person business that has never once deleted an e-mail could be sitting on top of several more terabytes of discoverable e-mails than a similarly-sized business with a consistently enforced 180-day e-mail retention policy. Reducing the amount of

\textsuperscript{14} Coleman at *7.

\textsuperscript{15} The jury verdict was subsequently reversed by the District Court of Appeals of Florida on other grounds. See Morgan Stanley v. Coleman (Parent) Holdings Inc., 955 So.2d 1124, 1126 (Fla. Dist. Ct. App. 2007).

ESI at the outset prior to litigation will pay dividends when it comes time to gather, process and review potentially relevant information.

When discovery turns to review of documents, just as with gathering ESI, the fewer gigabytes and terabytes of data to review, the lower the overall costs will be. This is significant when one considers that just one gigabyte of storage costs $0.20 to purchase and about $3,500.00 to review.\(^\text{17}\) If an ESI plan is functioning correctly – with the proper, identification, monitoring and disposal of ESI – a review will more likely involve necessary, easily identified data and thus maximize a corporation’s cost savings. With a poor or non-existent ESI management and retention policy, discovery costs can quickly snowball because of the necessity of reviewing a voluminous amount of documents in a considerably short time frame.

For instance, in *In re Fannie Mae Securities Litigation*, the Office of Federal Housing Enterprise Oversight (OFHEO) spent over $6 million on a review of 660,000 documents it was obligated to review in just a three-month period.\(^\text{18}\) To complete the extensive review by the court-mandated deadline, OFHEO hired over fifty contract attorneys solely for the purpose of reviewing documents that had been stored in back-up tapes and overlooked in the data gathering process. Despite its best efforts, OFHEO nevertheless missed numerous discovery deadlines and was ultimately sanctioned by the court for its failure to timely comply with its discovery obligations.\(^\text{19}\) While the court “appreciate[d] OFHEO’s effort to comply,” it concluded that OFHEO “ultimately failed to do so and [found] no abuse of discretion in the district court’s

---


\(^\text{18}\) 552 F.3d 814, 817 (D.C. Cir. 2009).

\(^\text{19}\) *Id.* at 818.
contempt finding or choice of sanction.\textsuperscript{20} Thus, a proper ESI retention policy that provides for a routine document destruction policy can narrow the scope of documents to be processed and reviewed. An ESI plan can reduce the costs associated with the review of potentially relevant material and can also help a company avoid sanctions for failure to meet important discovery deadlines.

In a study performed over a three-year period by the legal team of DuPont Corporation, it was discovered that fifty-percent of documents had been kept beyond their retention dates, resulting in over $12 million in needless discovery costs.\textsuperscript{21} While this study did not distinguish between ESI and non-ESI, the principle is the same: better management of information through routine and consistent practices can lead to substantial cost reductions at the time a company needs to review electronic materials for production.

**B. A Well-Prepared ESI Retention Plan Can Reduce the Burdens on In-House Counsel**

The litigation process is filled with perils for in-house counsel who are charged with appropriately preserving relevant documents when they receive notice that evidence is relevant to litigation or when they should know that evidence may be relevant to future litigation.\textsuperscript{22} When the duty to preserve documents arises and a business lacks an effective ESI retention policy, the possibility of making a mistake in meeting legal obligations dramatically increases. This failure to preserve relevant electronic documents can have severe consequences resulting in costly sanctions for a business. For instance, in *Qualcomm Inc. v. Broadcom Corp.*, the district

\textsuperscript{20} Id. at 816.


\textsuperscript{22} Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423 (2d Cir. 2001).
court ordered over $8.5 million in sanctions after the plaintiff failed to produce certain e-mails. Other severe sanctions, such as in *Zubulake v. UBS Warburg, LLC* 23 (*Zubulake V*) and more recently in *Pension Comm. of the University of Montreal Pension Plan v. Banc of America Sec., LLC* 24 permit the jury to make an adverse inference against parties who are found to be grossly negligent in their failure to preserve ESI. 25 Courts have even ordered imposition of fines, 26 the preclusion of evidence 27 and default judgment 28 as sanctions for mismanaged ESI.

Under Federal Rule 26, parties must disclose at the outset of litigation a description by category and location of ESI that it has in its possession, custody, or control, which it may use to support its claims or defenses. 29 A well-run ESI retention plan will have, well before litigation commences, identified a substantial part of a business organization’s ESI. An ESI plan can therefore assist a party to discharge its duty to make pre-trial disclosures at the very early stages of federal litigation. In *Phoenix Four v. Strategic Resources Corp*, a court imposed monetary sanctions on counsel who relied on the client’s statements about the location of relevant data and failed to conduct an adequate independent investigation. 30 The court further held that counsel had a duty to properly communicate with his client to ensure that all sources of the client’s information are discovered. 31 Notably, the court further advised that to discharge this duty,

---

25 Id. at 497-98.
30 No. 05 Civ. 4837(HB), 2006 WL 1409413 (S.D.N.Y. May 23, 2006).
31 Id. (citing *Zubulake V* at 432).
counsel should communicate with information technology personnel and the key players in the litigation to understand how electronic information is stored.\textsuperscript{32} To identify all sources of potentially relevant information, counsel should become fully familiar with a client’s document retention policies and data retention architecture.\textsuperscript{33} An ESI plan does not replace a counsel’s duty to investigate a client’s electronic information system, but it does bring counsel one step closer to understanding the client’s systems, processes and policies governing ESI.

In addition to helping make initial disclosures, Federal Rule 26’s meet and confer imposes another obligation that requires parties to participate in a formal meeting to draft a discovery plan.\textsuperscript{34} Federal Rule 26 mandates that at this meeting the parties discuss any issues relating to the preservation of ESI and develop a proposed discovery plan.\textsuperscript{35} Having a well-run ESI retention policy that anticipates litigation not only ensures that data may be identified easily but also that it is in accessible form for disclosure.

\textbf{III. HALLMARKS OF AN EFFECTIVE ESI RETENTION POLICY}

As discussed above, there are several significant cost benefits to maintaining a robust and effective ESI retention policy. However, there is no one-size-fits-all ESI retention policy and each policy will necessarily vary based on the organization.\textsuperscript{36} A company should nevertheless attempt to put together an ESI plan that meets various hallmarks of effective document retention plans. These hallmarks are present where a plan is: (1) reasonable; (2) tailored to the specific needs of a business organization; (3) clear about its document retention policies; and (4) consistently enforced and followed by a business organization.

\begin{itemize}
\item \textsuperscript{32} Id.
\item \textsuperscript{33} Id.
\item \textsuperscript{34} See Fed. R. Civ. P. 26(f)(2).
\item \textsuperscript{35} Id.
\item \textsuperscript{36} Sedona Guidelines, supra note 1, at 14 cmt. 2.a.
\end{itemize}
A. An ESI Retention Policy Should be Reasonable

First and foremost, a central hallmark of an effective ESI retention policy is reasonableness.\textsuperscript{37} Reasonableness depends on many factors, including the type of ESI and the circumstances under which the ESI is kept. Some factors to consider in developing a policy for ESI include the following: (1) nature of the business; (2) the legal and regulatory environment surrounding the organization and particular sub-units; (3) business culture; (4) existing data structure; and (5) existing ESI retention business practices that have evolved independently of any information management.\textsuperscript{38} A reasonable ESI retention policy will recognize and account for all these circumstances.

This standard of reasonableness does not mean that every piece of data within a business organization should be indefinitely preserved.\textsuperscript{39} As discussed throughout this article, it can be legally acceptable and often desirable for ESI to be destroyed at regular intervals. Technical, storage, and legal limitations often make retaining data for long periods of time unreasonable or unsustainable for business organizations. A reasonable policy will provide for the regular destruction of documents as well as consistent retention guidelines. The reasonableness of a retention policy with respect to particular ESI will depend on the circumstances in which the policy is being implemented. For example, in \textit{Lewy v. Remington Arms Co.},\textsuperscript{40} the court analyzed the circumstances of preserving certain categories of documents and found that a three-year period was not appropriate for all records. What constitutes a reasonable time to preserve ESI is

\begin{itemize}
  \item \textsuperscript{37} \textit{Id.} (citing \textit{Stevenson v. Union Pacific R.R.}, 354 F.3d 739, 747 (8th Cir. 2004) (citations omitted).
  \item \textsuperscript{38} \textit{Id.} at 14 cmt. 2.a.
  \item \textsuperscript{39} \textit{Zubulake v. UBS Warburg, LLC}, 220 F.R.D. 212, 217 (S.D.N.Y. 2005); \textit{Sedona Guidelines, supra} note 1, at 13 cmt. 1.c.
  \item \textsuperscript{40} 836 F.2d 1104, 1112 (8th Cir. 1988) (noting that retaining appointment books for three years might be reasonable, while retaining customer complaints about product safety for the same period might not be reasonable).
\end{itemize}
therefore dependent on many factors and circumstances that need to be weighed and analyzed by company management.

**B. An ESI Retention Plan Should be Tailored To The Company**

An effective ESI retention plan can be developed with a specific view toward the business organization’s specific needs, operations, information technology (IT) infrastructure and regulatory and legal responsibilities.\(^{41}\) Ideally, creation of a retention plan for ESI will be discussed and developed with input from legal counsel, IT representatives, records management representatives, and representatives from the business functions of the organization.\(^{42}\)

A very useful tool in developing a tailored ESI retention policy is creation of a comprehensive ESI data map, or ESI inventory, that details, among other things, the location, custodians, and types of ESI stored and used within a company.\(^{43}\) The first step in creating a data map should be to interview the heads of departments within a business organization to get an initial list of what kind of ESI is produced and stored within the business organization. This records inventory collects information about the organization that is relevant to the appraisal and retention determination that will have to be made with respect to different types of ESI.\(^{44}\)

Second, counsel should communicate with IT personnel to determine the storage and back-up systems used for the identified ESI. This information might include shared drives, local storage, back-up tapes and any other storage devices. Typical areas of a business organization’s system that should be accounted for in an electronic data inventory include:

- Network Servers

\(^{41}\) *Sedona Guidelines, supra* note 1, at 15 cmt. 2.b.

\(^{42}\) *Id.*

\(^{43}\) Conor R. Crowley, *Mapping Your Client’s Data*, 4th Annual Sedona Conference Institute Program on Getting Ahead of the eDiscovery Curve (Mar. 25-26, 2010).

\(^{44}\) *Sedona Guidelines, supra* note 1, at 11-12.
• E-mail Servers
• Desktop and Laptop Drives
• Software Services
• Back-up Data Systems
• Legacy Systems

However, ESI is not exclusive to these areas. When a party has notice of potential litigation, it has an obligation to preserve and produce ESI that is in its “possession, custody, or control.” Federal case law does not require legal ownership or physical possession for there to be “control” over ESI. ESI, such as electronic documents, may be considered under a party’s control when that party has the “right, authority or practical ability to obtain the documents from a nonparty to the action.” A company should consider the benefits of expanding its retention plan to include ESI that meets this criteria.

Once a comprehensive list of electronic information and its location is compiled, counsel should collect information on internal policies and practices that are in place with respect to ESI. For example, counsel should ascertain whether company policies permit users to save files, e-mails or other information to their desktop or laptop hard drives or removable media and the degree to which such practices comport with existing company policies.

---

45 *Crowley, supra* note 43 at 2-3.
49 *Crowley supra* note 43 at 2.
Once a business organization’s major repositories of ESI has been located and inventoried and all existing data management policies reviewed, the business should compile a complete data map. The data map should reflect, at least:

- Locations of Data
- Data Types
- Relationships to Other Data
- Retention periods

If properly prepared, a data map is a useful tool to analyze information flow and could aid in the identification of important electronic systems that may hold substantial amounts of business information. To make a data map relevant and useful once litigation occurs, it should be periodically audited and updated to reflect any changes to the data infrastructure of the organization.50 The more detailed a data map, the more helpful it will be in identifying all of the potentially relevant information that will need to be preserved and collected for review.

C. Developing a Clear ESI Retention and Destruction Schedule

An effective ESI retention policy does not simply identify and map data; it also sets each individual type of data to a specific retention and destruction schedule. This retention schedule dictates exactly how long certain data should be preserved before it is destroyed. It also details the policies and procedures for routine disposal of data that no longer provides value to the organization as well as litigation hold procedures that prevent any destruction of potentially relevant information in the event of litigation.

The first step before crafting either the retention schedule or policy is to analyze the value of the ESI stored within a business organization and determine to how long each type of data

---

50 Sedona Guidelines, supra note 1, at 43 (“Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.”).
should be retained. Basically, this is an assessment as to why a certain piece of data should be kept. Information without value should likely be purged. There are several different types of value or reasons for keeping data that should be assessed, including: (1) operational value; (2) vital record value; (3) regulatory value; and (4) fiscal value.

The operational value is assigned to records that are essential to the business of the organization. In other words, a company would desire to keep this information because it assists in carrying out its business purpose. For example, statistical reports could have a high operational value for an accounting firm or research notes may have a high operational value in a scientific laboratory. An obvious point worth making is that a company should be careful not to inadvertently call for the destruction of some information that is needed for the business to operate.

Vital records are documents that contain information necessary to recover and resume a business in the event of a disaster. These types of records generally have long retention periods. Examples of these records are licenses or tax documents that, if lost, could not easily be reproduced or recovered from any source.

Records with regulatory value are those that must be maintained to comply with legal requirements. In analyzing the legal value of data, an organization must be mindful of the different sources of law that might demand a production or use of this information such as: (1)
national-level statutes and regulations; state and local statutes and regulations; and (3) specific statutes of limitations of actions. Keeping ESI relevant to statutes of limitations may be necessary in cases where that information is needed as part of a legal defense, such as documents evidencing waivers or consent by certain parties. Since these statutes and regulations require various retention timelines, it is important for companies to particularize their retention treatment of various types of ESI to be in compliance with the law.

Fiscal records are important to consider because they relate to the financial transactions of an organization. For example, a fiscal record may include a document related to audit or tax preparation. Fiscal records may be valuable even if a business is no longer legally obligated to retain them because they may be necessary to maintaining a historical financial record for the company. Examples of such records include business ledgers, budgets, invoices, canceled checks, payroll records, and vouchers. This value too should be assessed in drafting a retention schedule.

After each piece of data has been analyzed, specific timelines for retention should be assigned to each type of data. As discussed above, several different values are assessed in determining how long to retain a piece of data. In conjunction with management and in-house counsel, records managers should assess each type of data, come to a retention determination and then draft a clear retention schedule to be distributed to the relevant custodians of documents.

---

56 For example, SEC Rule 17a-4 explicitly requires a three year e-mail retention period for all business communications related to broker-dealers. See 17 C.F.R. 240.17a-4. Also, a health insurance issuer offering individual health insurance coverage must maintain records for six years relating to the internal claims and appeals process. See 45 C.F.R. § 147.136.

57 Retention Management supra note 51, at 10.

58 Id.

59 Id.
within a business organization. A retention schedule should also be integrated into the business organization’s IT framework (e.g., automated back-ups, Microsoft Exchange server rules, etc.).

D. **Consistent Enforcement and Implementation of ESI Plan**

Retention schedules must be enforced within a business organization to be effective. To that end, the first task is the distribution of retention schedules and policies. Each employee assigned specific duties under the ESI plan should be notified of their responsibilities as soon as possible. ESI plans should also be made available in a central location (such as a company’s intranet site) for reference.60

Second, business organizations must ensure that policies are implemented consistently. As discussed above, inconsistent document retention policies are not viewed favorably by courts assessing a spoliation claim. Federal Rule 37’s safe harbor only applies to ESI lost “as a result of the routine, good-faith operation of an electronic information systems.”61 A fractured and non-routine policy will forfeit this protection in a claim of spoliation.

Implementing a routine and consistent ESI retention policy should include employee training. Employees should be regularly trained to comply with the business organization’s retention policy.62 This includes emphasizing retention protocols for new hires as well as current employees. Training should include instruction on how to retain ESI and how it must be disposed of in a consistent manner according to the retention schedule and policy.

Finally, a business organization should periodically audit compliance with its retention policy to ensure the policy is being consistently followed. After employees are trained, it is important to follow up and ensure that the ESI policies are being implemented properly.

60 *Sedona Guidelines, supra* note 1, at 41.
62 *Sedona Guidelines, supra* note 1, at 41.
Implementing an effective ESI retention policy requires full cooperation from all of a business’s stakeholders, including in-house counsel, IT personnel, management and employees.

IV. CURRENT E-DISCOVERY BEST PRACTICES AND SOFTWARE SOLUTIONS

Commercially available e-discovery software may aid in the process of implementing a robust ESI retention policy and greatly facilitate identification and preservation of relevant ESI. Many software solutions assist in expeditious location and identification of ESI, execution of litigation holds and collection of data. These software packages range in size from individual software modules tailored to specific e-discovery tasks to full-scale platforms developed for use with every stage of the discovery. Below is a brief overview of how commercial e-discovery software can aid in each of the major phases of ESI retention.

A. Identification

Many e-discovery vendors offer software solutions for the identification of ESI. Essentially, this software will track who is creating what data and where it is being stored.\(^{63}\) Thus, before litigation even begins, a business organization will have a clear picture of all the ESI currently being held. For the cost of a software license, businesses can be saved the enormous expense of having to hire IT specialists to wade through an organization’s network of computers and track down ESI. Many vendors offer this software as a stand-alone module and pricing is often based on the number of custodians in an organization.\(^{64}\)

B. Legal Hold

Another common e-discovery software solution is legal hold software. Legal hold software manages the implementation of legal holds as they arise from litigation. A typical legal

---


hold software solution will (a) send out notifications to all relevant custodians of the legal hold; (b) provide a questionnaire to be filled out by the custodian; and (c) report back in real time to the records manager on which custodians have acknowledged the legal holds as well as their responses to the questionnaire. Many legal hold software solutions, such as ZyLab’s legal hold software,65 will additionally make copies of all data under hold and preserve it on a central archive server.

C. Collection

Collection software enables a records manager to quickly grab and preserve ESI from across a business organization for such uses as early case assessment, review and production. For example, the EnCase eDiscovery software66 can cull the data set at the point of collection by targeting and collecting only necessary ESI based on keywords, hash values or any other file system metadata property.67 Furthermore, collection software often allows company employees to keep working while collection of ESI for litigation purposes is ongoing.

D. Scalability of Solutions

There are many e-discovery solutions that offer identification, legal hold, collection, and processing software as separate or all-in-one packages. A business can license from a single vendor for one of these solutions and cover each of these phases of ESI management. A business can adapt as much or as little software as needed to help it with its ESI retention needs and fit its budget. At the end of the day, it is important to remember that software, however used, is just one tool to implement an ESI retention policy and that participation from all sectors of a business organization is still very much needed.

67 Id.
V. CONCLUSION

A well-developed ESI retention policy increases efficiencies in the maintenance of ESI, reduces the costs of litigation and the risks of running afoul of e-discovery obligations. Implementing such an ESI retention policy in today’s business environment is not only good legal planning but also good business planning. A business without an ESI retention policy can put a company at risk of violating the duty to preserve evidence, federal statutes, state and local statutes, or administrative codes. The consequences of these transgressions can be severe. A company might have to pay steep sanctions in the form of fees and costs or risk adverse rulings from the court. Businesses may also be forced to spend significant resources to process and review poorly managed data, which can run into the millions of dollars. These outcomes can be mitigated with a robust and effective ESI retention policy. Ultimately, however, a business organization’s management, IT department, in-house counsel and employees are all responsible for ensuring that an ESI retention policy is executed in a consistent manner and in “good faith.”

The process of creating and implementing a comprehensive ESI retention policy may indeed take time and planning, but once in place should steer the business in the right direction as it navigates the e-discovery process.
Fernando A. Bohorquez is a partner at Baker & Hostetler and is a resident of the firm’s New York office. He focuses his practice on commercial litigation, intellectual property law and e-discovery issues. Mr. Bohorquez frequently lectures on e-discovery and handles a variety of matters in the field.

Alberto Rodriguez is an associate at Baker & Hostetler and is a resident of the firm’s New York office. He is a member of the firm’s commercial litigation and white-collar practice groups and has published several articles on e-discovery, social media and white-collar criminal law. Mr. Rodriguez is also part of Columbia Law School’s adjunct faculty and teaches a first-year workshop on legal practice.

Alan Pate, a summer associate at Baker & Hostetler, contributed to the preparation of this article.