

## GETTING YOUR E-DISCOVERY HOUSE IN ORDER

*By Diane Saunders, Jeffrey S. Siegel, M. Amy Carlin and Ron S. Allen*

According to a recent study, in 2006, the human race worldwide generated 161 quintillion bytes of information – or about 3 million times the information contained in all of the books ever written. Chances are, your company has contributed to the generation of digitally stored information. When you are facing litigation, you will be asked to comb through your electronically stored files, just as you would be expected to review your traditional paper files – however, that task may be more expensive, time consuming and difficult than simply reviewing file cabinets of documents.

In the electronic systems context, your company will face challenges when it is called upon to produce material that has been electronically stored, such as files maintained on computer servers, end user desktop and laptop computers, PDAs, blackberries, CDs, DVDs, memory sticks, etc. Your company should be knowledgeable about where its information is stored and what to do if that information becomes the subject of litigation. Unless your company has protocols that can be implemented quickly if an electronic discovery issue arises, it (and its counsel) is certain to face a struggle to adequately comply with the electronically stored information (“ESI”) preservation and disclosure requirements now required under modern court rules.<sup>1</sup>

As technology develops and businesses continue to rely more and more on electronic systems, ESI will become more important as it is likely to become a major source of evidence used by both sides in claims and lawsuits. Even as a third party, your company could be subpoenaed to provide ESI as part of the discovery process in a proceeding in which your company is not involved. “E-discovery” can be expensive, intrusive, and disruptive to your company’s operations. Preparation can minimize that expense, intrusion and disruption, and also help your company maintain more control over the process and avoid possible court sanctions in connection with the wrongful destruction of ESI.

This article will provide a guide for getting your e-discovery house in order so that your company will be prepared for electronic discovery issues when they arise. This article will suggest steps to consider to: (1) ensure your company knows which ESI it

---

<sup>1</sup> For more information on the e-discovery amendments to the Federal Rules of Civil Procedure, please visit MBJ’s legal updates at <http://www.morganbrown.com/legal/index.php>, and the articles contained in the archives. In particular, the following are instructive:

- CLIENT ALERT: Electronic Discovery and the New Amendments to the Federal Rules of Civil Procedure: A Guide For In-House Counsel and Attorneys  
<http://www.morganbrown.com/docs/FRCPP%20and%20E%20Discovery%20Newsletter.pdf>; and
- Electronic Discovery Update for Employment Lawyers  
<http://www.morganbrown.com/docs/MB&J%20Article%20-%20Electronic%20Evidence.pdf>.

maintains; (2) prepare your company so as to be ready to face e-discovery challenges; and, (3) minimize the cost and disruption of litigation in the electronic age.

✓ **CONDUCT AN INVENTORY OF HOW AND WHERE YOUR COMPANY'S ELECTRONIC INFORMATION IS STORED**

One of the important first steps towards discovery preparedness is to become familiar with and map out the intimate details and architecture of your information systems. Carefully inventory all relevant information systems so that key personnel can be clear about where and how potentially relevant ESI is contained in your company's systems. With a detailed road map of ESI, your company will not scramble to determine where information resides each time an e-discovery issue surfaces. If your company has the right to obtain documents from third parties, *e.g.* from independent contractors, be sure to include them on your inventory as well.

Beyond e-mail and word processing files contained on laptop and desktop computers, ESI can be stored on a number of other devices that your company may need to identify. For example, relevant data could be stored on devices such as: tapes, hard drives, zip drives, memory sticks, mobile telephones, handheld wireless devices, personal digital assistants, archive systems, and network servers. ESI comes in files of all shapes and sizes as well, including spreadsheets, power point files or other presentations, digital images, instant messages, audio and video recordings, data bases, graphics, and voicemail. Further, as technology continues to develop, there will be ever more devices on which to store information and formats in which it is stored, and therefore additional storage platforms subject to preservation obligations in litigation.

To begin to understand your company's computer systems, you should:

1. Chart out each storage device that your company uses, and what information is stored on each device;
2. List out the retention period currently used for all ESI; and
3. Identify whether any ESI is maintained on any back-up system and, if so, what the retention period is for the back up device.<sup>2</sup>

As part of your company's ESI inventory process, you should also become familiar with what the company will actually have to do to preserve the data. Identify the potential options for each system to alter preservation settings. (If you take these steps

---

<sup>2</sup> The accessibility of backed-up information should be assessed also. Accessibility should be a key component of your analysis because under the new amendments to the discovery rules, there is a difference between accessible and inaccessible data for the purposes of producing materials and allocating the costs of production among the parties. *See* Fed. R. Civ. P. 26(b). To place this in context somewhat, courts have typically associated producing data contained in back-up tapes as inaccessible data, and therefore susceptible to an argument for cost-shifting.

now, your company will be better able to respond to litigation holds, which are discussed below.)

Further, it is important to realistically assess your company's ability to perform this type of systems inventory without the assistance of an outside vendor. There are many outside vendors with expertise who are available to help your company inventory its systems and all the different preservation options available on those systems. An expert in systems architecture who is able to communicate effectively with your company's IT team can be an invaluable resource to utilize before your company is faced with an ESI issue that needs an immediate response.

✓ **ASSESS YOUR DOCUMENT MANAGEMENT AND RETENTION POLICIES**

Another important first step in getting your company prepared for e-discovery is to develop a concrete and consistent written document management and retention policy. A policy (or series of policies) serves two important purposes. First, it will assist you in identifying the company's storage needs while seeking to optimize operational efficiency. Second, the new federal e-discovery rules provide a safe harbor exception for a company that inadvertently destroys ESI. Consequently, a written retention policy may aid in demonstrating that the ESI at issue was lost in the course of the company's routine operation of its IT systems.

Your document management and retention policy should address all of the different kinds of ESI your company maintains (*i.e.*, documents, spreadsheets, e-mails, calendars, voicemail systems, etc.), the storage of such ESI and the timing for its retention. The policy should be implemented uniformly across the company to ensure that each unit or division of the company is retaining ESI for the same time periods.

In considering how long to store each type of ESI, your company should first consider whether any federal or state recordkeeping law applies. Generally speaking, laws regarding retention of records apply regardless of whether a record is maintained in paper or electronic format. Documents required to be retained by federal and state law have particular time periods for their retention. Additionally, your company will want to tie the period of retention of such files to the various and expected business need for the documents, as well as the history of the documents being subject to litigation. For example, a company may choose to retain electronic time records if it has a history of FLSA complaints and will want to rely on time records to defend such claims in the future.

Your policy should address storage media. Ultimately, your policy should be tailored to the needs of your ESI inventory, however, a partial list of items you may want to consider addressing include: determining how long e-mails should be archived on the hard drives of employee computers; instructing employees on the use of home computers;

determining whether to maintain prior versions of a final document; and, instructing employees on saving voicemails.

Companies, especially smaller businesses, are usually concerned that their capacity for storage will be adversely affected by retention policies relating to ESI documents such as e-mails and voicemails where the majority of communication between an employer, its employees, vendors and/or customers now occurs in this medium. Thus, companies often identify certain time periods necessary for the retention of such ESI. When considering whether a company has met its obligations for retaining e-discovery, some courts have looked to the size and resources of the corporation to determine when the storage of ESI information becomes a fiscal and administrative burden upon the corporation.

✓ **COMMUNICATE AND ENFORCE YOUR COMPANY'S DOCUMENT MANAGEMENT AND RETENTION POLICY**

While possessing a good document management/retention policy is essential, such a policy is meaningless without communicating it to your organization's personnel and educating them as to the importance of document retention and their role in ensuring that documents are retained. Also, make sure your employees are aware that all files on their company computers and portable storage devices belong to the company and could be implicated if an e-discovery issue arises.

✓ **CREATE A LITIGATION HOLD PROTOCOL AND A RESPONSE TEAM TO RESPOND TO THE LITIGATION HOLD**

Once your company understands what systems it has in place, you should then be prepared for what happens when a lawsuit (or threatened lawsuit) arises. A "litigation hold protocol" should set forth the steps your company will take when it has a duty to identify and preserve ESI. The purpose of creating such a protocol is to identify steps for the company to take once it "reasonably anticipates" litigation and once the obligation to preserve electronic evidence is triggered, *i.e.* once a "litigation hold" is necessary. Courts have defined the terms "reasonably anticipates" litigation in the context of the need to preserve evidence on a case-by-case basis. For instance, the duty to preserve evidence may arise as early as the receipt of an internal complaint of discrimination. At a minimum, the duty arises no later than the receipt of an administrative charge (*i.e.*, EEOC or DOL complaint) or the filing of a lawsuit. In many cases, the duty will arise before then.

In general, once the need for a litigation hold has been triggered, a company will need to take all reasonable steps to identify and retain all hard copy and digitally maintained files that may contain documents, correspondence (including e-mails), and records that may be relevant to the case. The creation of a litigation hold protocol provides a roadmap for the company to follow once the company reasonably anticipates

litigation. Because each company has its own systems, this article only addresses general steps to consider. Companies should work with their IT representative and outside counsel to refine these suggestions and develop practical, definitive steps in each situation. Further, depending on the situation and information available, you may wish to prioritize the suggestions below differently.

Specifically, in developing its litigation hold protocol your company should consider the following steps:

- Identify personnel to address e-discovery issues. Consider assembling a team including a manager, human resources representative, IT representative and counsel, who will meet regularly to ensure the protocol is followed. Identify who is the final authority on preservation issues. Within the group, you should identify a spokesperson who could testify clearly as to what steps you took to meet your e-discovery obligations.
- As cases come in, identify the key individuals who will have relevant information in this particular matter. For instance, in a discrimination case, the key individuals may likely be the supervisor/decision-maker, co-workers, and human resources representatives for the group. Also identify all systems which contain ESI (*i.e.*, servers, end-user computers, PDA's, blackberries, databases, etc.). Interview each key individual regarding potential sources of ESI.
- Transmit a notice to preserve information and to prevent deletion or destruction of e-mails or other ESI to all key individuals and IT personnel, *i.e.* a "litigation hold notice." It is prudent to either track receipt automatically or request recipients to acknowledge receipt by signing and returning a certification that the recipient has read the hold notice and understands the obligations contained within it.
- Gather information needed to quickly respond to information preservation letters and prepare for initial discovery planning discussions.
- Re-publish the litigation hold notice periodically to ensure compliance. In addition, the breadth of the hold notice should be expanded or narrowed to (i) target more precisely those employees who may have relevant information and (ii) identify relevant ESI. Consider re-publishing at least quarterly and/or when a major reorganization occurs within the company (especially in the IT department).
- Maintain an accurate log of all actions completed pursuant to your litigation hold. This log should be clear, concise, and available to the appropriate IT department personnel so as to minimize the risk that an IT

professional will overwrite this protocol (and, for instance, recycle back up tapes). The company should employ careful chain-of-custody procedures to any materials.

An essential component in the development of a response plan involves identifying key personnel who will be responsible for implementing the hold and ensuring that the necessary steps involved in preserving and producing relevant electronically stored information are completed. Such personnel should include a senior manager or executive, along with someone from information technology, human resources and possibly legal. Your “team” can then be responsible for implementing the response plan when the litigation hold arrives, and also for coordinating the e-discovery production.

✓ **CONSIDER WHO WILL PRESERVE ESI IN RESPONSE TO THE LITIGATION HOLD**

Depending on the IT infrastructure maintained by your business, there are likely to be many different options for your business to consider both in terms of *who* should be responsible for preserving the data in response to a litigation hold, and *how* it will be preserved. Determining who should be in charge of preservation and production, and what method(s) to use for the preservation of ESI during litigation, involves many competing concerns and will present many difficult questions for businesses and their counsel. Under the recent amendments to the federal rules, businesses and their counsel will be forced to address these questions very quickly after a case is filed.<sup>3</sup> While each case will require its own analysis, this section will highlight some of the key concerns and questions that businesses and their counsel should start thinking of as they prepare for electronic discovery.

A. *Your In-House IT Team*

Your in-house IT team is an obvious possibility to consider in determining to whom to delegate the responsibility of preserving and producing electronic data for litigation purposes. Relying on in-house resources can result in great cost savings for your business and can allow the business to exercise the maximum amount of control over the process. Where, for example, the data in question consists of highly confidential and proprietary business information, such as trade secrets, your company may be reluctant to involve outside consultants in the preservation and production process.

---

<sup>3</sup> Under amended Federal Rule of Civil Procedure 26(f), once a case is filed in federal court, counsel are expected to confer with each other in an effort to identify potentially relevant ESI and address issues of production of ESI. This conference is typically expected to take place within the first month or two after the case is filed. Amended Rule 16(b) further provides that the Court may, in its initial scheduling order, include provisions relating to e-discovery.

Relying on your in-house IT team can, however, sometimes present significant drawbacks. First, the added responsibility of identifying, preserving and producing electronic data can be extremely burdensome for and distracting to your IT team. Second, the members of your IT team, whose primary job responsibilities don't usually involve assisting attorneys with e-discovery, may not be as knowledgeable or as skilled as they should be to ensure that all of the correct data is preserved, or to determine the best methods for preserving the data. In order to effectively participate in the e-discovery process, your IT team will need to have a thorough knowledge of each system's architecture and of the various methods to preserve data from those systems. Your IT team will also need to be able to communicate effectively with case counsel, and be prepared to follow through on information requests from counsel in the short time frames set by the court. Unfortunately, not all in-house IT personnel may be as well-positioned as they should be to respond to an e-discovery issue when it arises.

In preparing for e-discovery, your company will be well served by assessing the knowledge and skill level of your IT team in terms of system architecture and preservation methods, as well as their communication skills. If concerns are raised, you should consider whether training would be beneficial and/or whether the company should look to develop a relationship with an outside consultant or vendor if an e-discovery issue arises.

#### B. *Outside Consultants*

For those companies that determine that their in-house IT team should not be burdened with the task of e-discovery, there are likely to be a variety of different consultants and vendors to whom they can go for assistance. The drawbacks of relying on outside sources to preserve and produce ESI are primarily the cost associated with such services and the loss of control over the process. The benefits of retaining the services of an outside firm specializing in the preservation and production of ESI can, however, sometimes be great.

Competent consultants who specialize in the preservation and production of ESI are knowledgeable about the e-discovery process and all the different options available to preserve and produce electronic data. Such consultants typically have the knowledge and communication skills to work with the company and company counsel to suggest the most cost effective strategies to obtain the results desired. They can also be relied on to focus on the project and are experienced working within the short time frames established by court rules for discovery.

If your company decides to utilize the services of an outside consultant, it is likely to be less disruptive to the company's IT department to work with a limited number of consultants, versus a different one for every case. Your company may also realize cost savings by utilizing one consultant as your company may be able to leverage its buying power by negotiating a lower, bulk rate with the consultant.

✓ **THINK AHEAD ABOUT THE BEST METHODS TO PRESERVE ESI IN RESPONSE TO A LITIGATION HOLD**

Not only are companies and their in-house counsel expected to understand the different preservation and production options so they can make effective decisions for the company when they are faced with e-discovery issues, in-house and outside counsel are expected by the courts to take an active role in the whole ESI preservation/production process to ensure that all discoverable information is preserved and searched, and to ensure that the company complies with its discovery obligations. Although a full discussion of the different issues that arise at the preservation and production stages are outside the scope of this article, the following issues should be considered.

A. *Metadata Issues*

“Metadata” is information which describes the characteristics of an electronic file. It is attached to a file and, thus, questions concerning metadata become complex. Will the metadata be preserved and/or produced? Does it need to be preserved and produced? In a sexual harassment case for example, it may be important to establish who received the complainant’s e-mail complaint of harassment, when it was received and to whom it was sent. Similarly, it may be important to note who edited the sexual harassment report, when the report was edited and the edits that were made. If the metadata is relevant to the case, it likely must be preserved and produced. Arguably, metadata is just like any other document and its relevance to the case must be disclosed like any other relevant document by counsel in the initial disclosures and discussed by counsel in the Rule 26(f) planning conference.

Metadata may, however, contain confidential, proprietary business information or even communications that are protected by the attorney client privilege, *e.g.*, where comments of an attorney are embedded in a Microsoft Word document. Depending on the nature of the metadata and the volume of documents, reviewing all the electronic documents and the accompanying metadata prior to production to make sure that no confidential and/or privileged material is inadvertently disclosed can be extremely burdensome and expensive.

In those cases where the metadata is determined to be irrelevant and is not sought in production, the electronic documents can be scrubbed of their metadata prior to production using scrubbing software, or produced in a searchable image format that does not include metadata, such as a PDF document. (Note: The metadata can still be preserved in case a determination is made later in the case that it is relevant, but it can be produced in a format that does not include metadata.)

In those cases where the metadata is determined to be relevant, your company will need to ensure that the metadata is preserved properly. While it may appear to be an

issue of simply copying the data in question to a separate file or even a server as a means of preserving and producing the data, if the proper methods aren't used to do so, the fragile metadata associated with electronic documents can be destroyed through the preservation process itself and court sanctions for the wrongful destruction of relevant evidence imposed. For example, the process of opening and saving a Microsoft Word document to another file as a means of preserving and/or producing the document will alter the metadata associated with that document that indicates when and by whom the document was last accessed, saved and/or modified. If your company decides to rely on its own resources to preserve and produce ESI, you will need to consider how your IT Department will deal effectively with the issue of metadata.

**B. *Physical Steps to Preserve Evidence***

There are a myriad number of ways a company may ensure the proper retention of ESI in response to a litigation hold. Your company should consult with both an IT professional and counsel to devise a realistic and effective strategy for preserving ESI once a litigation hold is necessary. ESI is very fragile. It can be modified in any number of ways – many times by accident. In addition, as discussed above, the metadata associated with the electronic files that need to be preserved can sometimes be destroyed through the preservation process itself if the proper methods are not used.

Once the ESI that must be preserved is identified, consider whether any of the following suggestions would ensure its preservation:

- Instruct employees to provide you with electronic copies of their relevant, active files. Users should be fully informed of the proper procedure for the capture and security of data (such as CD's, DVD's, memory stick, etc.). Users should be interviewed and the company should take an inventory of materials.
- Remove data from active servers (which are constantly being modified) to a secure, off-line server. While this may involve purchasing and maintaining a separate server, if your company anticipates frequent e-discovery issues, it may be a reasonable option to consider.
- Remove data from active servers to an off-line storage device. Copy relevant files from the source, *i.e.*, where it is currently stored, to off-line storage, such as to discs or other storage devices. Taking a complete forensic snapshot of the relevant employees' desktop computers, their e-mail mailbox on the work server and their mailbox and directories located on their laptop/home server can be a beneficial way to preserve documents that are typically and easily deleted by employees.

- If servers and other storage devices are backed up by using tapes, and such tapes are regularly recycled, it will be necessary to begin retaining the backup tapes to preserve backed-up files, and to discontinue any recycling of tapes that typically occurs.
- Create a backup of any applicable database to ensure that it is not overwritten or otherwise deleted. Consider creating a separate data backup that will be more easily accessible than a backup tape.
- Draft and enforce a policy requiring employee devices to be synchronized in order for the data and ESI on these devices to be stored in default on a separate server. In the case that voicemails are saved or deleted, they should also have a separate server. This relevant ESI should then be transferred to a secure site for preservation.
- Direct employees to save their work-related files with a separate accessible location (*e.g.*, create separate e-mail folders that store e-mails related to a specific topic or project). When the project is completed, the e-mails can be saved as a document on the main server and with the other ESI documents relating to that specific project. This ensures that, at a minimum, the e-mails are sorted and easy to locate.
- Turn off any automatic deletion function for “key individuals” who own, generate, or receive relevant e-mails. If your IT system has a strict limit on the size of an individual’s mailbox, turn off the limit as it applies to any “key individual.”
- Consider taking a complete forensic snapshot of “key individual’s” data – including their computer, their server-located mailbox, and server-located home directory. Consider whether the “snapshot” should be in native form so as to preserve metadata.

✓ **THINK AHEAD ABOUT PRODUCTION ISSUES**

A. *Form of Production*

The fragile nature of ESI, its metadata and the sheer volume of electronic documents can present production issues that do not arise with the production of paper documents. Once you have identified the relevant ESI and its retention, you should start thinking ahead about how you will produce the ESI to your opposing party when the time comes. There is no best format that works in all cases, and the party requesting the ESI can specify, under the new rules, the form in which he or she wants the ESI. The value and expense of the different production methods will need to be weighed in each case to determine the best and most cost effective production method for that case.

For example, when documents in discovery are voluminous, it is normally desirable and is the generally accepted practice to bates stamp, *i.e.*, affix document numbers on, the documents in order to be able to identify who produced the document. Bates stamping also prevents tampering with the documents, which can be accomplished very easily when electronic documents are produced in their native format. However, bates stamping documents in their electronic format can be expensive and requires that the documents be converted from their native format into a format that prevents altering and allows some type of numbering. Your company may need to rely on outside resources in connection with the production of ESI and may realize cost savings if it is able to negotiate a bulk arrangement ahead of time with such a provider.

B. *Attorney-Client Privilege and Confidentiality Issues*<sup>4</sup>

Ideally, each party will not mistakenly produce privileged or confidential materials. Instances may arise, however, where because of the large amount of ESI produced, a document may be inadvertently disclosed to the other side.

Recognizing the burden and expense imposed by conducting extensive pre-disclosure reviews of voluminous ESI for privilege and confidential information, the new amendments include several provisions that attempt to recognize the burden and cost of conducting privilege/confidentiality reviews on large quantities of ESI. For example, the rules include a provision whereby privileged electronic documents that are inadvertently disclosed can be returned to the disclosing party without, presumably the attorney-client privilege being waived. *See* Rule 26(b)(5)(B). The rules also include several provisions that make clear that the parties are free to come to agreements themselves about how to handle privilege issues and that the court can incorporate the parties' agreement in its scheduling order provisions. *See* Rules 26(f) and 16(b)(6).

One type of agreement is a "claw-back" agreement whereby the producing parties can produce documents after a screening process and, if the producing party determines that it has inadvertently produced privileged or other confidential material, it can demand the return of the privileged document. Another such agreement is a "quick peek" agreement whereby the producing parties can produce large quantities of unscreened documents for initial review by the other side, the reviewing side can then designate documents for production and the producing party can then conduct a privilege/confidentiality review of those designated documents.

Both of these options, as well as the privilege procedure included in the new amendments, can result in great cost savings since they narrow the need for extensive

---

<sup>4</sup> For a more detailed discussion of attorney-client issues, please refer to: *Advancing Technologies, Advancing Ethics - The Impact of Communication Technologies on Attorney Ethical Obligations*, <http://www.morganbrown.com/docs/Advancing%20technologies-ethics.pdf>, available at MBJ's website, legal updates: <http://www.morganbrown.com/legal/index.php>.

privilege/confidentiality reviews of voluminous materials. However, there is an open question as to whether the attorney client privilege will be deemed to have been waived through such agreements even when they are included in a court order pursuant to Rule 16(b)(6). The new amendments to the Federal Rules of Civil Procedure do not change the relevant substantive law on the attorney-client privilege waiver in the particular jurisdiction in which the case is pending. Ultimately, you should work with your counsel to address privilege issues in the context of e-discovery.

✓ **COORDINATE WITH LEGAL COUNSEL**

Communicating with your legal counsel in the course of preparing for the new landscape of e-discovery is crucial. When litigation ensues and preserving and producing ESI becomes a real issue, it will be necessary for your counsel to be aware of your information systems, and to be able to work with you in coordinating your litigation hold and your e-discovery production. You will need to be prepared to deal with all aspects of records management -- identifying systems, preserving and collecting records, analyzing what is relevant in each case and producing records in discovery. Counsel can assist you in tweaking your plan in advance so as to preclude potential difficulty when the time comes to execute your response plan. As with most business issues, an ounce of prevention is worth a pound of cure.

MBJ is prepared to work with you and your IT professionals to address e-discovery issues both before they arise and in connection with a particular matter. Please contact any of the authors of this article or your regular MBJ attorney to discuss how to best implement these strategies within your company.

---

*Diane Saunders, Jeffrey S. Siegel, M. Amy Carlin and Ron S. Allen are members of the firm's e-discovery task force. They, like all attorneys at Morgan, Brown & Joy, LLP, may be reached at (617) 523-6666 or by visiting [www.morganbrown.com](http://www.morganbrown.com). Morgan, Brown & Joy, LLP focuses exclusively on representing employers in employment and labor matters.*

This publication, which may be considered advertising under the ethical rules of certain jurisdictions, should not be construed as legal advice or a legal opinion on any specific facts or circumstances by Morgan, Brown & Joy, LLP and its attorneys. This newsletter is intended for general information purposes only and you should consult an attorney concerning any specific legal questions you may have.