

COPING WITH E-DISCOVERY UNDER THE NEW RULES

DISPELLING THE MYTHS – IT'S NOT AS
COMPLICATED AS YOU THINK

John Michael Raborn

GMWD

Gibson, McClure, Wallace & Daniels L.L.P.

Gibson, McClure, Wallace & Daniels, L.L.P.

8080 N. Central Exp.

Suite 1300, LB50

Dallas, TX 75206

SUMMARY

The issue of *electronically stored information* (ESI) and its relation to discovery entered the legal scene over ten years ago. We now call it “e-discovery,” but many do not understand how it works. Indeed, to understand e-discovery, knowledge of how computer systems operate is necessary. Unless you have taken relevant classes or have taught yourself the topic, the odds are you do not know how the computer, cell phone, or blackberry you use every day truly functions. By reading this article, you will gain an understanding of e-discovery.

A quick look at ESI sheds light on the complexity and variety of issues surrounding e-discovery. The volume of ESI for a company, or even an individual, is far greater than paper information. For example, the average employee sends or receives fifty messages (emails, text messages, instant messages, etc.) per day. Thus, a company with 100 employees has approximately 1.2 million messages per year. The storage of data further complicates retrieval of information. ESI may be located in numerous places, such as hard drives of different computers, company servers, home computers, and backup tapes. Backup tapes store an exact copy of data so information can be recovered if there is a problem with the system. It is the volume of, and difficulty in locating, ESI that makes e-discovery such a daunting task.

This article will examine:

- What should and should not be produced;
- The scope of electronic discovery;
- The associated costs of retrieving electronic discovery;
- How electronic information is obtained;
- The party’s duty to retain electronic information (and, likewise, when there is no duty);
and
- What happens if electronic information is destroyed or deleted, either accidentally or on purpose.

I. INTRODUCTION

On December 1, 2006 the amendments to the Federal Rules of Civil Procedure, regarding the discovery of *electronically stored information* (ESI), went into effect. Businesses and lawyers alike have been scrambling to understand the amendments and act accordingly. This article outlines how the amendments affect the discovery of ESI and provides suggestions on how to prepare for the issues arising from the amendments.

Because of the complexities associated with electronically stored information, companies need to be proactive in sorting through the issues. As explained below, knowledge is the key. Get to know your computer systems and where different types of ESI are stored. It is also important to establish a records-management policy. Such a policy operates to delete, reuse, and recycle storage space.

II. WHEN THERE IS A LAWSUIT: IDENTIFYING “ELECTRONICALLY STORED INFORMATION” THAT MIGHT NEED TO BE PRODUCED

a. What is “ESI” and Why is it Important?

The type of electronically stored information is identified by its location, which often dictates whether it is discoverable. Active data, information located in a computer system’s memory or in storage media attached to the system, is considered accessible to the user. Systems data, which includes information regarding when users logged on and off, applications used, and websites visited, is likely to be more remote. Other types of data, such as deleted files and data located on backup tapes, are much more remote and require the assistance of a computer specialist to locate.

The amended language of Federal Rule of Civil Procedure 26(a)(1) replaces “data compilations” with “electronically stored information,” which clarifies the party’s duty to include ESI in disclosures. However, with regard to less-accessible ESI, the Rule provides that a party is not required to “search back-up systems or to retrieve deleted files in an exhaustive effort.” As this rule pertains only to disclosures, it may be necessary to retrieve less-accessible ESI for subsequent discovery.

Importantly, the amended rules do not create a duty to produce ESI that is inaccessible. However, like paper documents, less-accessible ESI may require production if a court determines it is relevant to the “subject matter involved in the action” and is for “good cause.” The new rules mandate early meetings between parties for the purpose of easing the complications of e-discovery. Parties are encouraged to sort through easily accessible ESI to determine whether less-accessible ESI should be searched.

b. Metadata Associated with Documents in Electronic Form – Who, What, When, Where, and Why?

“Metadata” is information about a data set or specific document that describes how, when, and by whom the data set or document was created, modified, accessed, or collected. Metadata

from an email provides information about the history of its transmission. Thus, a blind-copied recipient may not be as disguised as the author intended. Some metadata is easily accessible to users while other metadata is hidden on the operating system or processing program. Some metadata is unusable when the data to which it is linked is removed from the creating system. For example, certain metadata of a document created in Microsoft Word but produced in portable document format (PDF) cannot be discerned. The reason is because a PDF is essentially a photo of the original document, and the photo does not capture metadata relating to the original.

III. ALLOCATION OF COSTS – WHO PAYS THE BILL TO RETRIEVE ELECTRONIC INFORMATION?

If a producing party is not able to accurately provide information regarding where particular ESI may be located, a court is more likely to order that party to conduct costly searches of a variety of sources. In the alternative, a court may order the producing party to bear the cost of having a third-party vendor, selected by the court, search the party's networks and systems. In essence, the offending party is forced to incur double the fees of searching its ESI.

Awareness of and familiarity with information systems allows a producing party to accurately disclose what may be on a less-accessible source at the outset of litigation. If it is determined necessary for a producing party to search a less-accessible ESI source, some of the cost may be shifted to the requesting party. It is important to note that many businesses outsource their computer management and data-storage functions. A third party in this instance may also be required to produce ESI.

IV. FORMS OF PRODUCTION FOR ELECTRONIC INFORMATION

ESI can be produced in a number of formats, including "native format," the form in which it was created, or PDF, an electronic photograph of the document. A requesting party is permitted to designate a format, but a producing party may, under valid objection, produce in a different format. Many attorneys do not recommend producing ESI in native format because native files are easy to alter, metadata may change in the production process, formats may inadvertently change upon production, and it can be inefficient to produce numerous documents in a variety of formats.

V. PRESERVATION AND SPOILIATION – WHAT IS A PARTY'S DUTY TO PRESERVE ELECTRONIC INFORMATION?

a. The Duty to Preserve

The duty to preserve ESI arises only when future litigation is reasonably anticipated, or should be anticipated. In order to effectively preserve ESI, companies should become familiar with:

- How employees use computers;
- What information is available on the computers and systems;
- What routine operations occur and how they change information; and
- The individuals with the most knowledge of the computer and programming systems.

b. Implementing Litigation Holds to Suspend Destruction of Electronic Information

Once the above questions are answered, it will be easier to initiate “litigation holds” when the duty to preserve arises. A litigation hold is the suspension of routine information destruction policies to ensure relevant documents are preserved. A properly implemented litigation hold may allow the data producer to preserve ESI before a lawsuit is filed. Courts have said that ESI made by or for “key players” in the lawsuit requires preservation. Key players are those close to the issues or incidents made the basis of the claim. Key player ESI on less-accessible storage devices, such as backup tapes, may require production due to the relevance of the data.

The courts indicate the duty to preserve extends to all relevant ESI in existence at the time the duty to preserve arises, and includes all data made by or for the key players. If it is necessary to implement a litigation hold, we recommend notifying all employees involved in the subject matter of the lawsuit of the hold, specifically communicating directly with the key players. As a precaution all relevant, accessible backup tapes should be identified and stored safely.¹

Spoliation is “the destruction or significant alteration of evidence or the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.” ESI gives rise to new spoliation concerns because computer systems automatically recycle and reuse memory space. This means a user unintentionally deletes or alters potentially relevant information. In fact, a digital file is altered simply by opening it.

For purposes of a litigation hold, the question of when litigation is reasonably anticipated can be difficult. For example, does the company reasonably anticipate litigation when one employee overhears a co-worker discussing how her boss made sexual advances toward her? One court indicates a company cannot reasonably anticipate litigation simply because one or two employees contemplate the possibility that a co-worker may sue. Thus, a company-wide duty to preserve does not arise. But consider the situation where an executive contemplates litigation after receiving an attorney’s demand letter from a former employee – a court is likely to consider that the company has notice. In that instance, the duty to preserve information arises, and a litigation hold should be implemented with regard to relevant information concerning the termination of said employee, specifically, relevant information made by or for key players.

Temporary data creates another unique spoliation issue. A computer’s random access memory (RAM) is blank when a computer is first turned on. During the use of the computer, different information is stored on the RAM. When the computer is turned off, the RAM is wiped clean. Some companies implement a record-retention plan so that information stored temporarily on RAM is preserved in a usable form. Other companies, however, do not have a preservation plan. Some courts say that such companies do not have a duty to change their policies when litigation is reasonably anticipated; but if preserving such information is as easy as “flipping a switch,” a court may be compelled to order a party to do so. This is based on the courts’ tendency to order production of ESI which requires little effort, but not where greater effort is needed.

¹ Generally, a litigation hold does not extend to inaccessible backup tapes – those typically maintained solely for the purpose of disaster recovery.

VI. RECORDS MANAGEMENT – WHY “SPOILIATION” CAN BE A FOUR LETTER WORD

Another issue finding its way to the courthouse concerns records-management policies. One function of a records-management policy is to delete certain information on a scheduled and ongoing basis (e.g. purging e-mails and recycling backup tapes). Thus, the problem becomes whether the deletion of relevant data was done pursuant to an established records-management policy or under order of the litigation-fearful user. In order to protect the user whose files have been deleted pursuant to a records-management policy, Rule 37(f) provides: “*absent exceptional circumstances*, a court may not impose sanctions . . . for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

This rule does not protect users who conveniently implement a records-management system prior to, or at the outset of, litigation. Further, a routine, wide-spectrum file deletion policy is frowned upon and may warrant sanctions. In a recent case between an employer and recently-terminated employee, the employer argued that it had a routine practice to wipe the hard drive of computers used by recently-terminated employees. The court ruled against the employer because the “routine” practice was not consistently applied to other terminated employees. Further, the employer had reason to believe litigation would arise as a result of the termination and, therefore, had a duty to preserve data. It is important to note that the phrase “absent exceptional circumstances” gives courts flexibility. In other words, a court may order sanctions even against a party whose files were deleted pursuant to a routine and good-faith operation of its system if the “exceptional circumstances” so warrant.

If a court determines a party is guilty of spoliation it may impose sanctions. For example, a court may instruct a jury to infer that deleted evidence would have been unfavorable to the party responsible for the deletion. Such an instruction is used when a court determines the destructing party 1) had an obligation to preserve the evidence, 2) had a culpable state of mind, and 3) the evidence was relevant to a claim or defense.

When data is wiped because it is not necessary for business purposes, like RAM, a court is not likely to issue sanctions for failing to retain said information because its deletion lacks willful action. Where requesting parties seek temporary information, they must be assertive in their approach, such as seeking a preservation order.

Although courts understand the difficulties of e-discovery, sanctions will be issued when necessary. In fact, if a lesser sanction does not suffice, a court may dismiss the case with prejudice against the offending party. For such a dismissal to be warranted, it is likely a party committed a number of violations or a single gross offense. Sanctions can be avoided by increasing familiarity with ESI and e-discovery, and by taking appropriate precautions.

VII. E-DISCOVERY IN EMPLOYMENT LITIGATION

Employees need to understand that their daily work may be important to potential litigation in which the company may become involved. Equally important is that the employees be informed

of how ESI can affect their employment status and potential litigation between the employee and employer. For example, employees' e-mails, internet history, blogging, and instant messages may be relevant to litigation. In fact, even employees' personal computers or cell phones may have ESI that is discoverable. One example is where employees use their cell phones to text message each other outside of work.

Inclusion in the employee handbook of policies governing use of the employer's communication systems is ideal. It is also sound practice to include ESI information in the employer's discrimination policy. Language such as "inappropriate use of electronic communications" will put employees on notice that their electronic communications can be the basis of discrimination. Many employees fail to realize that their communications, even if electronic and outside the office, can be relevant to, or the subject of, litigation. Furthermore, to protect themselves, companies should implement guidelines for their Information Technology specialists. One such guideline would be to report to Human Resources any unauthorized or inappropriate ESI or electronic communications. Further, implementation of an internet usage policy is critical because an employer on notice of illicit internet use has a duty to investigate.

VIII. AT THE END OF THE DAY . . .

The question is often posed – which cases require a serious look into these e-discovery issues? It appears the answer is: any case where computer use is relevant. In the employment context, if a terminated employee brings a wrongful termination claim, any ESI regarding the employee's employment is relevant. Perhaps the employer is arguing the reason for termination was for sexual harassment, specifically, where a co-worker received inappropriate text messages or instant messages from the terminated employee. The relevant ESI of the key players (terminated employee, co-worker, and those making the adverse employment decision) is discoverable. Remember, inaccessible or even less-accessible ESI may avoid production, but a party should make an attempt to accurately describe all ESI. Also, where complete tangible documents are properly produced, the relevant ESI may avoid production. The reality is that it does not seem to make a difference how "big" a case is. If ESI is relevant, it is discoverable.

Whether it is the IT department or an appointed team, individual knowledge of systems, location of ESI, and how to collect ESI is crucial. Further, these individuals should be able to testify on these issues. Implement and document an ESI preservation process. The more you, as a company, know about e-discovery, the more you will be able to work with your in-house or outside counsel. This should not only help to contain costs, but you may establish a good faith defense by donating time and effort to managing ESI.

GMWD

Gibson, McClure, Wallace & Daniels L.L.P.

Gibson, McClure, Wallace & Daniels, L.L.P.

8080 N. Central Exp.

Suite 1300, LB50

Dallas, TX 75206