Oregon Law Institute
of Lewis & Clark Law School

The Changing Face of Commercial Litigation

Friday, September 26, 2008
Oregon Convention Center
777 NE Martin Luther King Jr. Blvd.
Portland, Oregon

Chapter 1

AVOIDING THE PITFALLS OF ESI SPOLIATION

Keith A. Ketterling
Angelene Carpenter Falconer

Table of Contents

NOTES

Chapter 1

AVOIDING THE PITFALLS OF ESI SPOLIATION

Keith A. Ketterling
Angelene Carpenter Falconer

I. INTRODUCTION

The goal of this chapter is to discuss changes in commercial litigation with regard to spoliation of electronically stored information ("ESI") and to provide you with practical steps you can take to avoid e-discovery disputes. Due to its format, ESI is especially vulnerable to deletion, modification or corruption and parties and counsel must take extra precautions to preserve this type of evidence. We will discuss the obligations of the parties and their counsel in dealing with ESI, how the courts handle spoliation, and how to prevent and detect spoliation.

IT personnel, previously in behind-the-scenes roles, will find themselves front and center in the e-discovery process. However, the burden to meet the challenges posed by ESI is not solely on the parties. Counsel and e-discovery vendors are facing direct liability for failing to adjust their practices to changes in the rules regarding ESI. The courts expect litigants and their counsel to take a proactive approach to identifying and preserving all sources of potentially relevant information, and greater expectations will transfer to vendors as well. Amendments to discovery rules are now years old and judges are less tolerable of failures by parties, as well as their counsel and vendors, to discover and produce electronic documents.

II. OBLIGATIONS TO PRESERVE ESI, INCLUDING METADATA

A. Obligations of Counsel[1]

1. Once the potential for litigation is apparent, it is counsel's obligation to implement a "litigation hold," notice given by a party's in-house or outside counsel that litigation is likely or has commenced and that the parties must preserve all potentially relevant information. However, it is not sufficient to place the litigation hold and expect parties to retain and produce the relevant information. In addition to placing the hold, counsel must oversee compliance with the litigation hold, monitor the parties' efforts to retain and produce all relevant information and periodically reissue the hold throughout the litigation.

2. Counsel has an obligation to become fully familiar with his or her client's document retention policies and computing infrastructure. Communicating directly with "key players" and IT personnel to identify and preserve all sources of potentially relevant information, including backups, is mandatory.

B. The Parties

1. The obligation of the parties to preserve ESI is the same as for other types of evidence. However, its format makes ESI more susceptible to spoliation, and

---

[1] *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (SDNY 2004), provides very explicit guidelines for parties and counsel in future litigation to follow regarding the discovery of ESI.

therefore parties must be particularly cautious to preserve the integrity of this type of evidence. Not only is the content, or the face, of electronic documents relevant, but the metadata, the "data behind the data," such as information about who created the document and when it was created, last modified or printed, may be even more important to proving claims or defenses in a case.

a. Once litigation is reasonably anticipated, and certainly once counsel has issued a litigation hold or the court has ordered one, the parties are obligated to discontinue all data destruction, and parties would be wise to also discontinue the recycling of backups. (See *Zubulake* at n. 72 regarding backup tapes.)

b. Parties must preserve and not dispose of relevant hardware unless exact replicas of the files (mirror images) are made. Software is available to create exact duplicates of hard drives so that all metadata is preserved. IT personnel and vendors performing this work must carefully document this process and be prepared to testify regarding the steps taken to preserve the integrity of the data and the chain of custody.

c. Parties must maintain all pertinent information and tools needed to access, review and reconstruct the data. (If certain data is only viewable with a specific software program, parties must maintain that program so that the data may be examined).

2. A party may also have potentially relevant ESI stored on its behalf by third parties, such as vendors or contracted consultants. These third parties are under the same obligation as the plaintiff or defendant to comply with the litigation hold issued by counsel and to preserve any data or software that may be relevant to the claims or defenses of the lawsuit.

III. UNINTENTIONAL, NEGLIGENT, RECKLESS OR WILLFUL SPOLIATION

1. Individuals and businesses cannot be expected to maintain the terabytes of data that can accumulate over time, and ESI is often recycled or overwritten in the normal course of business. A party's unintentional failure to provide ESI that is destroyed during "the routine, good faith operation of an electronic information system"[2] is protected from sanctions by the federal rules.

2. However, once litigation reasonably is anticipated, counsel must implement a litigation hold, communicating directly with key players, IT personnel and any third parties, and instructing them to suspend routine system operation to prevent the loss of potentially relevant information. Parties and their counsel may be liable for spoliation if those routine processes are allowed to continue, negligently or recklessly destroying information that they should have preserved. If the party reasonably believes that relevant information may exist on backups and that information is not available on more easily accessible sources, the duty to preserve applies to those backups as well.

---

[2] Rule 37 Advisory Committee Notes, 2006 Amendment, Subdivision (f)

3. In addition to parties and counsel, vendors can get caught up in discovery disputes and find themselves with liability issues as well. Mismanaged document processing, inadequate searching or production glitches can lead to unintentional non-production of relevant and discoverable documents or inadvertent production of privileged information.[3]

4. Surprising examples of intentional non-production or willful spoliation of information can be found, demonstrating complete disregard for the discovery rules and even court orders. Some of the most blatant cases warranting sanctions are discussed in Section IV below.

IV. SANCTIONS

A recent survey of sanctions awards by Hon. Shira A. Scheindlin and Kanchana Wangkeo concluded that a finding of bad faith is not necessary to impose sanctions for spoliation of ESI, and often sanctions are aimed at simply restoring an injured party to the position the party would have been in but for the spoliation. However, where willful conduct or bad faith is present, courts may award sanctions even without proof of prejudice. In the majority of the cases surveyed, courts considered both the intent of the spoliator and the prejudice to the moving party.[4]

1. A court recently sanctioned a party $8.5 million in fees and costs, and referred six attorneys to the state bar for investigation. Specifically, the discovery abuses included failing to access and review some of the key witnesses' computers, failing to use a list of search terms, which easily could have been compiled with the help of the prejudiced party, to identify relevant documents.[5]

2. Often, courts try to remedy a party's disadvantage by imposing an evidentiary sanction, such as precluding a party producing relevant emails after the discovery cutoff from using any of the emails at trial, but allowing the disadvantaged party to use them during its case.[6]

3. Judges may also attempt to mitigate the damage by granting an adverse inference instruction to the jury, telling jurors that they are allowed to infer that the destroyed evidence could have been damaging to the spoliator. A judge recently awarded this sanction against a party for failing to produce documents that had been in the physical custody of a contracted third party.[7]

---

[3] *Victor Stanley, Inc. v. Creative Pipe, Inc., et al.*; 250 F.R.D. 251 2008 WL 2221841 (D. Md. 2008).

[4] Shira A. Scheindlin and Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 Mich. Telecomm. Tech. L. Rev. 71 (2004), *available at* http://www.mttlr.org/voleleven/scheindlin.pdf.

[5] *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. January 7, 2008), vacated in part by 2008 WL 638108 (S.D. Cal. March 5, 2008).

[6] *Thompson v. U.S. Department of Housing and Urban Development*, 219 F.R.D. 93 (D. Md. 2003).

[7] *Nursing Home Pension Fund v. Oracle Corporation*, Slip Copy 2008 WL 4093497 (N.D. Cal. 2008).

4. A court may impose a sanction of dismissal or default judgment if there is no other way to cure the prejudiced party[8] or to protect the integrity of the judicial process.[9] The courts reserve this penalty for only the most egregious violations. If a party has destroyed important computer data, leaving the adversary no way of prosecuting or defending its case, or if a party has routinely violated discovery rules and disobeyed court orders, a judge may ward the ultimate sanction of dismissal or default judgment.

V. PREVENTION

1. Implement document retention policies and train employees to follow them. Keeping documents for only as long as necessary for business and/or legal reasons and destroying or recycling outdated documents according to your company's policies can reduce exposure. Of course, once litigation reasonably is anticipated, automatic destruction or recycling of any potentially relevant documents is sanctionable.

2. Implement a hold as soon as litigation is anticipated and advise all employees and any third party consultants to suspend document destruction and recycling activities. Attorneys may be sanctioned for failing to inform clients of their obligations and not clearly communicating to them their responsibilities to preserve potentially relevant evidence, including electronic documents.

3. Early involvement with "key players," IT staff, paralegals and even experts can be critical for identifying and preserving potentially relevant information. Leaving no stone unturned does not mean that every piece of information in the whole universe of a party's documents must be preserved, but a good faith effort to ensure that no relevant information is lost is required by all parties.

4. Meet and confer with opposing counsel. Transparency with adverse parties and the court about efforts to identify and retain potentially relevant information can prevent disputes. In addition to following the practices above with regard to your own clients, it can be helpful to communicate with opposing counsel early in the litigation, outlining your expectations that all parties will follow the same rules, and inviting them to enter into a conversation with you on how to proceed with discovery.

    a. Send a letter to the adverse party or opposing counsel putting them on notice that they should already have a litigation hold in place, and outlining in detail the types of information you expect to be preserved.[10]

    b. Rule 26A disclosures fell out of fashion with parties taking advantage of the option to waive them. However, they can be a very effective tool with e-discovery. Use the opportunity to exchange lists of search terms and "key

---

[8] *Playball at Hauppauge, Inc. v. Narotzky*, 745 N.Y.S. 2d 70 (N.Y. App. Div. 2002).

[9] *Mariner Health Care, Inc. v. PricewaterhouseCoopers LLP*, 638 S.E.2d 340 (Ga. App. 2006) (state court's order dismissing the case with prejudice reversed and order imposing sanctions nullified because plaintiff filed for dismissal without prejudice minutes before the sanctions hearing against it).

[10] See Stoll Berne sample letter to opposing counsel, "Notice of Duty to Preserve," attached.

players," including IT personnel. IT personnel will likely be the ones responsible for searching and preserving electronic documents, and could have very valuable information about sources of information, accessibility of those sources, retention policies, backups, etc., especially if spoliation is a concern. (Any issues about confidential and proprietary information could be addressed with a protective order.)

c. Use the Rule 26F conference as an opportunity to discuss the expectations of the parties, including the types of documents you anticipate seeking in discovery and the format in which those documents should be produced.

5. Involve the court and/or appoint a special e-discovery master. Requesting a status conference with the judge may be enough to prompt a hesitant adversary to join you in a discussion about how to proceed with discovery. Demonstrating an effort to cooperate may help you defend an allegation of spoliation later on.

6. "Monitor and adjust" relates to continuing involvement with clients, vendors and paralegals as discovery develops. Sources of information that may not have seemed likely to contain relevant information early in the litigation may suddenly become important, and the sooner you take steps to limit any unintentional destruction of relevant information the better you'll be able to defend an allegation of spoliation.

VI. DETECTION

1. Demand native review of electronic documents if spoliation is suspected. For example, the properties of a native PDF produced by a party may show that it was created with a word processing program many months after the date shown on the face of the document and that the signature is an electronic image copied and pasted from another document. If the party had only provided a TIFF image or a paper copy of the document, none of this information could have been discovered and the forgery could have been submitted to a jury in support of a breach of contract claim.

2. Involve experts to help mirror exact duplicates of hard drives, preserving the integrity of documents' metadata. It is advisable to mirror the hard drives of key players who are likely to have large amounts of relevant documents on their machines as soon as litigation is anticipated. Proving a negative may be impossible if extensive destruction has occurred. However, even "scrubbed" machines may still contain data that can provide vital information about files and folders that no longer exist, and often even deleted documents and fragments can be restored or recovered.

3. Invest in litigation support software to gain more control over your work product or rely on vendors to house and produce your documents. There are many case organization tools available at a wide range of prices. These programs can help you search and catalogue your case documents, allowing you to keep pace with the large amount of data that can be produced in a complex commercial case. If you don't have the resources to manage these tools in house, vendors can host databases for you, giving you remote access to documents stored on their servers.