BUSINESS LITIGATION BASICS

E- Discovery

James C. McMichael, Jr.

McMichael, Medlin, D'Anna, Wedgeworth & Lafargue, L.L.C.

P. O. Box 72

Shreveport, Louisiana 71161-0072

Phone: (318) 221-1004

Fax: (318) 221-0008

jmcmichael@mmw-law.com

December 17, 2020

I. Early E-Discovery case law

Zubulake v. UBS Warburg (S.D.N.Y. 2003)

For all intents and purposes, the rulings in the Zubulake cases put e-discovery on the map. On its surface, Zubulake was an unexceptional employment discrimination case. Then it was discovered that the defendants deliberately destroyed electronic evidence and demonstrated little care in preserving potentially relevant documents. In a series of groundbreaking rulings, U.S. District Judge Shira Scheindlin levied heavy sanctions for the destruction of evidence, fundamentally changing the way lawyers and organizations look at e-discovery. The Zubulake decisions (there were five separate ones in total) tackled a host of issues that hadn't previously been addressed by any federal court, establishing important new standards that precipitated the FRCP e-discovery amendments, including:

• The scope of a party's duty to preserve electronic evidence during the

course of litigation

• Lawyers' duty to monitor their clients' compliance with electronic data

preservation and production

• The ability for the disclosing party to shift the costs of restoring "inaccessible" electronically stored information (ESI) to the requesting party

• The imposition of sanctions for the spoliation (destruction) of electronic evidence.

Wilson v. Thorn Energy, LLC (S.D.N.Y. 2011)

In this case, the defendants discarded a flash drive, which had held financial documents that were relevant to the case after determining that data stored on the drive could not be read. The judge ruled that the defendants' failure to preserve and produce documents in a timely manner constituted gross negligence. The case reaffirmed the preservation standards established by Zubulake exposed the challenges and complexities associated with preserving certain types of ESI, an issue that continues to resonate today.

Mt. Hawley Ins. Co. v. Felman Prod., Inc. (S.D. W. Va. 2010)

While the two prior cases mainly centered on preservation issues, Mt. Hawley exposed the emerging risks using technology to search through vast amounts of data. After a software indexing issue contributed to Nearly 400 privileged emails being produced, the judge ruled that the error resulted from the plaintiff's failure to "perform critical quality control sampling." This ruling allowed documents containing particularly damaging attorney-client privileged information to be entered as evidence. It continues to serve as an important reminder that while technology has an invaluable role in the e-discovery process, it can't be used as a shield against e-discovery mistakes.

Da Silva Moore v. Publicis Group (S.D.N.Y. 2012)

Another case involving e-discovery technology, U.S. District Judge Andrew Peck's decision in Da Silva Moore was the first to formally approve the use of technology assisted review (commonly referred to as predictive coding) software that takes information entered by people and applies it to a larger group of documents, making the review process much quicker, not to mention more accurate. Since the Da Silva Moore ruling, predictive coding has been used in a number of cases and is widely viewed as a highly effective means for identifying relevant documents and reducing the cost of review.

II. 2006 Federal Rules Amendments

The 2006 FRCP amendments cover five related areas:

(a) definition of discoverable material;

(b) early attention to issues relating to electronic discovery, including the format of production;

(c) discovery of electronically stored information from sources that are not reasonably accessible;

(d) the procedure for asserting claim of privilege or work product protection after production; and

(e) a "safe harbor" limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems. FRCP 16 - In a nutshell, this rule basically requires that attorneys come into pretrial conferences with at least some knowledge of the client's IT and data environment, so they can begin to discuss the scope of discoverable ESI.

Definition of Discoverable Material

The amendments introduce the phrase "electronically stored information" to Rules 26(a)(1), 33, and 34, to acknowledge that electronically stored information is discoverable. The expansive phrase is meant to include any type of information that can be stored electronically. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

Early Attention to Electronic Discovery Issues

Several of the amendments require the parties to address electronically stored information early in the discovery process, recognizing that such early attention is crucial in order to control the scope and expense of electronic discovery, and avoid discovery disputes. Rule 26(a)(1)(B) adds electronically stored information to the list of items to be included in a party's initial disclosures. Rule 16(b)(5) adds provisions for the disclosure or discovery of electronically stored information as an item that may appropriately be included in the court's scheduling order. Rule 26(f) expands the list of issues that must be discussed as a part of the meet and confer process, and includes a requirement that parties develop a discovery plan that addresses issues relating to the discovery of electronically stored information – including the form or forms in which it will be produced. It also requires parties to discuss any issues relating to the preservation of discoverable information, and address issues relating to claims of privilege or work product protection.

Format of Production

Amended Rule 34(b) addresses the format of production of electronically stored information, and permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The rule does not require the requesting party to choose a form of production, however, since a party may not have a preference or may not know what form the producing party uses to maintain its electronically stored information. The rule also provides a framework for resolving disputes over the form of production, in the event that the responding party objects to the requested format(s). Finally, the rule provides that if a request does not specify a form of production, or if the responding party objects to the requested form(s), the responding party must notify the requesting party of the form in which they intend to produce the electronically stored material – with the option of producing either (1) in a form in which the information is ordinarily maintained, or (2) in a reasonably usable form.

Electronically Stored Information from Sources that Are Not Reasonably Accessible

Amended Rule 26(b)(2) creates a two-tiered approach to the production of electronically stored information, making a distinction between that which is reasonably accessible, and that which is not. Under the new rule, a responding party need not produce electronically stored information from sources that it identifies as not reasonably accessible because of undue burden or cost. If the requesting party moves to compel discovery of such information, the responding party must show that the information is not reasonably accessible because of undue burden or cost. Once that showing is made, a court may order discovery only for good cause, subject to the provisions of the current Rule 26(b)(2)(i), (ii), and (iii).

Asserting Claim of Privilege or Work Product Protection After Production

The addition to Rule 26(b)(5) sets forth a procedure through which a party who has inadvertently produced trial preparation material or privileged information may nonetheless assert a protective claim as to that material. The rule provides that once the party seeking to establish the privilege or work product claim notifies the receiving parties of the claim and the grounds for it, the receiving parties must return, sequester, or destroy the specified information. The rule does not address whether the privilege or protection is waived by the production, but simply prohibits the receiving party from using or disclosing the information, and requires the producing party to preserve the information, until the claim is resolved.

Safe Harbor

Under Rule 37(f), absent exceptional circumstances, 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. Generally, the routine operation of an electronic information system refers to the ways in which such systems are generally designed and programmed to meet the party's technical and business needs, and includes the alteration and overwriting of information that often takes place without the operator's specific direction or awareness.

However, the protection of Rule 37(f) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith. A party cannot exploit the routine operation of an information system to evade discovery obligations by failing to prevent destruction of stored information that it is required to preserve.

III. Louisiana's response to the case law and the 2006 Federal Rules Amendments

Various provisions of the Louisiana Code of Civil Procedure were amended to reflect the changes to the 2006 amended Federal Rules. Amended Louisiana Code Civ. P. 1462 parallels the protections of Fed. R. Civ. P. 26 that "a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."

If a court nonetheless orders discovery, the court "may specify conditions for the discovery," such as limiting its scope. The party seeking discovery may specify "the form or forms in which information, including electronically stored information, is to be produced," but "[i]f objection is made to the requested form or forms for producing information …or if no form was specified in the request, the responding party shall state in its response the form or forms it intends to use."

Rule 1462 was invoked in the case of Louisiana Workers' Compensation Corp. v. Quality Exterior Services, L.L.C., 92 So. 3d 1034 (La. Ct. App. 1st Cir. 2012). In that case, the Court rejected plaintiff's argument that defendant's discovery request for documents to be produced in their native format as not reasonably accessible because of undue burden or cost such that plaintiff could avail itself of the protections of Rule 1462. Calling the plaintiff's reasoning "circular," the court concluded that the alleged undue burden and inability to produce information capture on a

2005 year-end back up tape did not preclude it from producing any available information regarding a 2008-2009 policy-year audit. In addition, plaintiff's argument that defendants would not "understand" information produced natively was not a sufficient basis upon which to disallow production.

Amended Rule 1471(B) reproduces the safe harbor protection of Fed. R. Civ. P. 37(e) in that, "[a]bsent exceptional circumstances," sanctions may not be imposed for failure to provide electronic evidence destroyed as a result of routine, good-faith operation of electronic systems.

Amended Rule 1424(D) offers similar protection embodied in Fed. R. Civ. P. 26(b)(5) from inadvertent waiver of the attorney-client privilege when there were reasonable steps taken, and prompt notification of the disclosure. Although this provision does not expressly refer to ESI, it was adopted after the influence of the 2006 federal amendments, along with the other ESI-specific provisions.

Art. 1424(D) clawback provision states that "[a] disclosure of a communication or information covered by the attorney-client privilege or work product protection does not operate as a waiver if the disclosure is inadvertent and is made in connection with litigation or administrative proceedings, and if the person entitled to assert the privilege or work product protection took reasonably prompt measures, once the holder knew of the disclosure, to notify the receiving party of the inadvertence of the disclosure and the privilege asserted. Once notice is received, the receiving party shall either return or promptly safeguard the inadvertently disclosed material, but with the option of asserting a waiver. Even without notice of the inadvertent disclosure from the sending party, if it is clear that the material received is privileged and inadvertently produced, the receiving party shall either return or promptly safeguard the material, and shall notify the sending party of the material received, but with the option of asserting a waiver."

Amended Rule 1460 follows the amended Fed. R. Civ. P. 33(d) option to produce, or rather permit inspection of ESI business records in response to interrogatories. Article 1461, which, like Fed. R. Civ. P. 34, allows for entry to inspect records, was likewise amended to address ESI. The plain meaning suggests that the responding party would provide the requesting party with such access The rule provides in pertinent part that "[w]hen the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information … or from an examination, audit, or inspection of such business records … and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit, or inspect such records and to make copies, compilations, abstracts, or summaries. A specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained." From a strategic standpoint, the remote access option is likely one parties would be reluctant to utilize).

In the case of electronic information, Article 1462(E) contemplates that the responding party will make the initial attempt to search its own devices for discoverable information. If dissatisfied, the requesting party may then move to compel inspection of the responding party's devices when the responding party has failed to respond properly to a request to produce electronically stored information. In bringing this motion, the requesting party has the burden of establishing good cause:

If the requesting party considers that the production of designated electronically stored information is not in compliance with the request, the requesting party may move under Article 1469 for an order compelling discovery, and in addition to the other relief afforded by Article 1469, upon a showing of good cause by the requesting party, the court may order the responding party to afford access under specified conditions and scope to… inspect, copy, test, and sample the designated electronically stored information within the scope of articles 1422 and 1425.

The 2007 Revision Comments accompanying art. 1461 explain that an order permitting inspection of an adversary's computers should be granted when the requesting party has shown good cause that the initial production of electronically stored information was not in compliance with an appropriate discovery request.

Louisiana courts have often looked to federal cases for guidance in interpreting state procedural rules that are similar to the Federal Rules of Civil Procedure. Ogea v. Jacobs, 344 So.2d 953 (La. 1977); Madison v. Travelers Ins. Co., 308 So.2d 784 (La. 1975). To that end, several federal courts have ordered inspections of physical files and computers so long as there is no undue burden on the producing party and safeguards are put in place to prevent the disclosure of confidential and/or privileged documents. See, e.g. Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) (Information stored in computer format is discoverable, so long as producing party is protected against undue burden and expense and/or invasion of privileged matter by implementation of a Court-ordered protocol); Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002) (cost of mirror imaging defendants' computers would be borne by the plaintiffs; however, if any defendant elected to conduct a full privilege review of its e-mails prior to production, that defendant would do so at its own expense); Simon Prop. Grp. L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000) (Plaintiff was entitled to attempt to recover deleted computer files from computers used by employees of defendant, whether at home or at work, to develop evidence supporting plaintiff's claims; however, protective measures would be taken, including plaintiff's appointment of an expert who would serve as an officer of the court and turn over the recovered information to defendant's counsel for appropriate review prior to production); Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645 (D. Minn. 2002) (Motion to compel inspection of computer records and appointment of neutral expert in computer forensics to retrieve and examine the records granted pursuant to established protocol).

However, see Memry Corp. v. Ky. OilTech, N.V., 2007 WL 832937 (N.D. Calif. 3/19/2007), in which the Court stated that a mere desire to check that the opposition has been forthright in its discovery responses is not a good enough reason to permit inspection of the opponent's computers..

IV. Preservation of data - the Legal Hold

The duty to preserve evidence begins or is triggered when a party knows of, or has a reasonable anticipation of future litigation. The legal hold itself is simply a notification, usually sent over email, stating that a lawsuit has been commenced or is reasonably anticipated and that the party receiving the email must preserve all data potentially related to the subject matter of the case. A defensible legal hold process includes periodic reminders, compliance monitoring and other considerations as matters evolve.

When do you send the legal hold?

A legal hold should go out immediately once litigation commences or can be reasonably anticipated, such as an acrimonious employee dismissal or product defect that will almost surely prompt litigation.

Who sends the legal hold?

The legal hold should come from in-house or outside counsel who should be responsible for managing the process. Counsel is often assisted by paralegals or e-discovery managers, who specialize in the nuances of day-to-day legal hold management, and who don't need extensive legal training to perform the job effectively.

Who do you send the legal hold to?

The legal hold should go to anyone who might possess potentially relevant electronic information.

What goes in the legal hold notification?

There is no specific legal requirement for what goes into a legal hold notification. That being said, an effective legal hold communication will clearly and succinctly establish the specific electronic or paper documents that need to be preserved, using things like names, dates, and underlying issues of the matter. It should also make clear the legal necessity and include an easy way for the custodian to get in touch with the issuing lawyer if they have any questions.

Receipt of a Preservation letter

Another preservation trigger is the receipt of a preservation letter, a communication sent from one party to another notifying them of their preservation obligations and conveying what must be retained. Preservation obligations kick in regardless of whether a preservation letter is sent or not, and it is not a substitute for an actual lawsuit or court order. Although preservation letters are not a formal component of civil discovery procedure, they are commonly used.

It is not sufficient to simply notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Rather, affirmative steps must be taken to monitor compliance so that all sources of discoverable information are identified and searched. To accomplish this, "reasonable steps" that must be taken, including: (1) "Becoming fully familiar with the document retention practices, as well as the client's data retention architecture"; (2) Identifying "key players" and "sources of discoverable information"; (3) Putting "in place a

litigation hold and making that known to all relevant employees by communicating with them directly"; (4) Repeating the litigation hold instructions "regularly"; (5) "Monitoring the compliance so that all sources of discoverable information are identified and retained on a continuing basis"; (6) "Calling for employees to produce copies of relevant electronic evidence"; and (7) "Arranging for the segregation and safeguarding of any archival media (e.g. backup tapes) that [the client] has a duty to preserve.

Failure to Preserve

Judges have a significant amount of discretion when it comes to penalizing parties for spoliation of evidence. In assessing the severity of sanctions, courts will generally focus on two key areas: (1) the level of culpability (was the spoliation intentional or simply the result of negligence?) and (2) the relevance of the evidence (was the spoliated evidence central to the arguments of the case or more on the periphery?). Minor sanctions include monetary fines or attorney compensation. When the failure to preserve is determined to be intentional and involves highly relevant evidence, sanctions become much more severe and can include adverse jury instructions, whereby the jury is instructed to infer that the lost evidence was unfavorable to the spoliating or default judgments, where the court will actually issue a ruling against the spoliating party for failing to comply with the discovery requirements.

V. Collection of data

Methods of Collection

There are a variety of ways that organizations approach the collection process. Questions that dictate the collection methodology include:

How much data is involved in the legal matter?

How many sources of data are implicated, and how accessible are those data sources?

Will the collection involve any specialized tools or expertise?

Does the legal matter involve encrypted or sensitive data?

Are there internal IT resources available to perform/assist with the data collection?

What are the time constraints (production deadlines, retention schedules, etc.)?

What type(s) of collection technologies are deployed to perform the collections?

Employee Self-Collection

Employee self-collection involves letting the custodians themselves copy relevant files into a shared drive or portable storage device. Most experts advise against employee self-collection pointing out that most employees aren't technically savvy and are highly likely to make mistakes

and overlook key documents. For small matters involving low volumes of highly conventional data (email, word processing documents, etc.) employee self- collection may be reasonable and cost effective, especially when the opposing party and judge have signed off on the plan ahead of time.

Internal IT collection

By far the most common collection approach, IT collection involves members of the IT department performing the actual data collection at the direction of the legal department.

External IT Collection

For organizations with very limited IT resources, a third-party expert might be called on to perform the data collection. An outside expert is likely to have set procedures and all the necessary tools and skill to perform a collection that will withstand the highest levels of judicial scrutiny.

Remote Collection

These collections employ a centralized internal collection system that is integrated with company data sources allowing for electronic information to be collected remotely. Though the collection might still be performed by an IT professional, it doesn't require any direct interaction with the data sources themselves and can usually be performed much quicker and more efficiently than with traditional methods.

VI. How collection of data works in real life

The goal of IT collection is to achieve targeted collections of data and information by applying search and analytics technologies. This is typically achieved through the use of the identification of specific search terms, specific custodians and specific date parameters used to quickly and accurately locate relevant documents.

Parties in litigation can agree to the entry of an order setting forth an E-Discovery protocol that can establish the general parameters of production of electronic information, including how the documents are to be produced, how duplicate documents are to be dealt with, whether and to what extent metadata is to be included in produced documents, etc. Such protocols address the requirement that parties limit themselves to a reasonable number of search terms per custodian per party and upon reasonable and relevant date ranges per custodian to which the search terms will be applied. The protocol usually includes the general goal that the search terms be narrowly tailored to particular issues and proportional to the needs of the case. The needs of the case are weighed by considering the importance of the issues at stake, the importance of the discovery in resolving those issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

To the extent that there are no protocols agreed upon or if agreed upon, that there are contested requests for additional or fewer search terms or for more or fewer custodians, or there is a claim that the requests will generate too many documents or are not proportional to the needs of the case, the Court can step in and resolve the disputes based on the principles of reasonableness stated above.

Another method of identifying electronic documents is predictive coding or technology aided review (TAR). Predictive coding is a relatively new concept in the legal world, although machine learning algorithms exist all around us. It's how our email systems filter spam messages from our inboxes and how websites are able to pepper us with advertising tailored to our specific browsing habits.

Not so simply explained, in predictive coding reviewers pull a representative cross-section of documents, known as a "seed set," from the full population of documents that need to be reviewed. Reviewers then code or label each document in the seed set as responsive or unresponsive and input those results into the predictive coding software. The software then analyzes the seed set and creates an internal algorithm or formula for predicting the responsiveness of future documents. Users sample the results of the algorithm on additional documents and refine the algorithm by continually coding and inputting sample documents until they achieve desired results.

Courts have recognized that these technologies are used in cases with large volumes of documents and indeed should be left to the producing party's discretion. See Da Silva Moore v. Publicis Groupe & MSL Grp., 287 F.R.D. 182 (S.D.N.Y. 2012) "What the Bar should take away from this Opinion is that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review."; Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, (S.D.N.Y. 2015) acknowledging that "[i]n the three years since Da Silva Moore, the case law has developed to the point that it is now black letter law that where the producing party wants to utilize [TAR] for document review, courts will permit it. While Judge Peck cautioned parties about the need to be transparent with their seed set development, he also noted that there are other means to evaluate the efficacy of predictive coding without agreeing on seed set parameters, including manual sampling of coded documents.