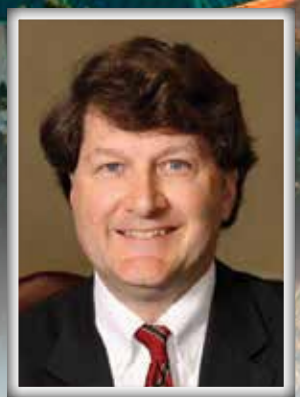
ALABAMA DEFENSE LAWYERS ASSOCIATION

JOURNAL

Spring 2015 • Vol. 31 • No. 1



Michael E. Upchurch
Mobile, Alabama
President 2015-2016

ANNUAL MEETING
June 18-21, 2015 ~ Sandestin Golf and Beach Resort, Baytowne

BIBB ALLEN MEMORIAL TRIAL ACADEMY
August 6-7, 2015 ~ Cumberland School of Law

IT'S ALL ELECTRONIC DISCOVERY

By: Paul Zimmerman

Anyone who has taught a child how to ride a bicycle knows that most kids start riding without realizing that no one is holding onto the bike anymore. In other words, the child is riding and does not even realize it. Similarly, litigators are conducting electronic discovery, but simply may not realize it and have been successful in deluding themselves into thinking that they do not (or do not need to) conduct electronic discovery. Once litigators realize that they are already involved in electronic discovery, then it is not so scary (just like the child realizing that she's riding all on her own). The next step is to become more competent and more capable.

The goal of this article is to assist attorneys in their electronic discovery practice. This goal is reached by first helping litigators realize that they are already riding the bike. This article will discuss some basic tips, particularly for smaller cases, and provide resources for continued development of electronic discovery practice. This article discusses the "small" case common in litigation, involving maybe a handful of computers, and with relevant players that have cell phones.

The context of this article is very important. As explained later, proportionality analysis, such as pursuant to Ala.R.Civ.P. 26(b)(2)(B), is key. What is considered appropriate or reasonable in the "small case" may not be, and indeed, probably is not, appropriate for the "big case." Much of what is in this article is not scalable and will not apply to all situations. For example, while "self collection" will be acceptable in many cases and for many litigants, large or more sophisticated institutional clients may not act reasonably in self collecting, and it may not be appropriate when wrongdoers (such as rogue employees) may try to delete data. Never lose sight of the possible need to meet higher standards, whether in discovery practice or, almost assuredly, in regulatory investigations. But for now, continue on, even if it is with training wheels.

We are already conducting electronic discovery

Electronic discovery is not just teams of contract lawyers sitting in a review center in some unknown location, reviewing millions of documents in a class action employment suit against a multi-national corporation. It is not just the production of hundreds of thousands of documents in native format collected from a virtual server, the restoration of back-up tapes, or the harvesting of an entire data base. Electronic discovery is simply discovery involving information stored on a computer or memory device.[1] If the case involves devices and media such as email, computer files, spreadsheets, text messages, Gmail, or a smartphone, it involves electronic discovery.

Many attorneys confuse the form of production with electronic discovery and say that they "avoid electronic discovery." That is probably not really what they mean, given that discovery must certainly include information stored on computer and memory devices. Rather, most attorneys who speak of "avoiding" electronic discovery are generally referring to the form of production, and simply elect to produce (and agree to accept) either paper documents or static PDF images. And for many cases, the production of hardcopy documents or static images (e.g., PDFs), is fine.

But it is time to stop thinking that we are "avoiding electronic discovery" simply by not producing documents in electronic form or hiring an electronic discovery provider. The bottom line is that assisting or advising clients concerning relevant emails, Word documents, spreadsheets, pictures on a camera phone, or when there is a possibility that relevant text messages were exchanged or messages were posted on social media, *is* electronic discovery. It really is that simple, and it is nothing to avoid. Indeed, ethical duties prohibit the avoidance of e-discovery if relevant information is stored electronically.[2] It is essentially impossible in this age to conduct litigation without handling electronic discovery—it is only a question of handling it correctly.

Start to finish, electronic discovery is the "process of identifying, locating, securing, and producing" information stored on a computer or memory device.[3] Of course, to be able to conduct more thorough electronic discovery, the attorney must adequately interview the client and discuss the related issues with opposing counsel (and often non-parties). Taking the right steps generally will not happen without asking the right questions. In the same way that much of the computer world may be foreign to the attorney, it could be foreign to the client as well. Not only that, but even if the client understands the technology and the issues that relate to electronically stored information ("ESI"), the client will need assistance with understanding how legal burdens and implications affect how the client's ESI is handled within the context of litigation.

Simple steps to better managing electronic discovery

The very first step in managing electronic information in a case is to explore the data potentially involved to the same degree as the merits of the case. Two duties affect the attorney's work here: (1) the duty of competence under Rule 1.1, and (2) the duty to conduct a reasonable inquiry under Rule

26. Use a checklist in the course of this discussion to ensure that nothing is omitted and to document the discussion in case an issue of spoliation arises later.[4] Checklists used in discussions with the client should be comprehensive, just like checklists used in other areas. This can make the checklist a bit intimidating for some attorneys. Simpler checklists are available and could be used in cases that are simple in terms of sources of data, types of data, volume of data, etc., but they obviously increase the risk of omitting relevant information.[5] All aspects of electronic discovery start with an understanding of the data and the sources of data involved in the case, and that is generally only discovered by accident (if at all) if it is not specifically discussed with the client early in the case.

It All Starts with Preservation

Next, always undertake preservation efforts. Though many lawyers and parties in litigation are frequently concerned about spoliation sanctions, they are fortunately rare.[6] If data is preserved, the chance of sanctions for spoliation are essentially nil, though failing to produce ESI or altering it along the way are still potential problems (and sanctionable).

The law requires reasonable efforts in preserving evidence.[7] Allowing the client to take steps to search for, identify, and preserve relevant information is known as "self preservation." In many cases, self preservation may be permissible as reasonable efforts, particularly in small cases, where the data involved is simple and not voluminous, and the capabilities of taking reasonable efforts to find and identify relevant data can be demonstrated. There are certainly circumstances under which self preservation or self collection is not reasonable, particularly if the party does not have sufficient resources by which to preserve and collect data without altering it in a way that affects the case, or a clear incentive to allow evidence to be lost can be shown. Obviously, self preservation or collection is not without risk and must be weighed within the context of the case.

Attorneys have a duty to advise their clients regarding the preservation of evidence.[8] This is nothing new. However, what is new with electronic data is that it can be extremely fragile. Historically, documents were kept in filing cabinets, and those cabinets were often locked or kept in a locked office. While the impetus and ability to destroy relevant evidence has always existed, accidental loss of evidence has historically been less of an issue in most cases than it is today, because short of a fire or a flood where the documents are stored, they were generally available. Today, that evidence may be on a laptop computer, which is subject to having a drink spilled on it, or on a smartphone, which can fall out of a pocket or get left on top of a car at any time. Furthermore, thumb drives get lost all the time. Careless loss of data should be prevented. Obviously, parties or reluctant witnesses can "delete" computer data at the touch of a button, thereby requiring forensic computer analysis and a measure of luck to recover it. Furthermore, the volume of hardcopy information, both relevant and not relevant, was limited and in an understandable filing system. ESI is voluminous and is not always organized and stored in a manner understood by most people.

While the duty to preserve evidence can be statutory, regulatory, or even contractual,[9] the most common source of a duty to preserve relevant evidence is a reasonable anticipation of litigation. Once a duty to preserve relevant data is triggered, litigants must take reasonable efforts to preserve data that is potentially relevant to the litigation.[10] The date on which litigation was reasonably anticipated can be different for the different parties, since it is often not triggered for the defendant until the defendant is served with the summons and complaint.[11] Various indicators of a reasonable anticipation of litigation can be an EEOC charge,[12] a demand letter from an attorney, or a greater than usual internal investigation by the (potential) defendant.

Preservation is a process that requires a system and monitoring. It is not a one-time event (i.e., the litigation hold memo), and most courts impose on counsel a duty to assist clients in preservation efforts and to then monitor compliance.[13] Preservation begins with counseling the client on the client's obligations regarding preservation and assisting the client in those efforts, including identifying, locating, and protecting relevant data.[14] Must we always send a written litigation hold letter to our clients? Not under Alabama law.[15] Is it the prevailing best practice? Absolutely. Stated otherwise, can it be said that the best practice is to rely upon a verbal litigation hold instruction? No. Consider how simple or comprehensive to make a written litigation hold, but regardless of the complexity of the case, the data, or the environment containing the data, the hold notice should be clear, understandable, and as concise as possible, with practical instructions. With institutional clients, inquire as to the preservation efforts to date and whether the client is looking to outside counsel to take the lead in those efforts. Document the discussion. Take into account past engagements, if any. Set reminders/ticklers to send periodic written reminders to the client given the commonly imposed duty of counsel to supervise preservation efforts.

Instructions for a litigation hold, whether written or verbal (which must be documented in the file), must inform the client: (a) how to determine what data is relevant; (b) what type of data must be preserved; (c) how to preserve it; (d)

what to do with it; and (e) must advise the client to continue preserving new data generated subsequent to the litigation hold.[16] Enough information about the litigation must be provided in order to allow the client (and its employees, if the client is an organization) to discern what information is potentially relevant. While it is possible to simply request that the client preserve all information, in whatever form, regarding a certain event, person, or period of time, this is probably overly broad and imposes a hardship on the client in a number of ways. Automatic deletion of relevant files and email must be suspended.[17] Consider whether self preservation/collection of documents by the client is reasonable (i.e., defensible) in the case at hand or whether a vendor needs to be involved in those processes. The hold notice should contain contact information for questions, additional information, or assistance. Determine whether to preserve data in place or require collection of potentially relevant data to ensure against spoliation, either intentional or otherwise.

Pull back-up tapes for relevant time periods out of rotation if they might contain relevant evidence. Do not forget about text messages and other more obscure or personal data sources, such as tablets, thumb drives, online repositories (such as the employee who emails documents to himself via Gmail to work on the weekend), etc., or personal devices owned by employees that were used for work. And of course, social media is ubiquitous and must always be explored as possible data sources, especially as to the employees involved in the controversy. Again, given the mind boggling (and every increasing) types and sources of data, checklists are a must.

Many courts in the 11th Circuit have held that counsel has a duty to monitor clients,[18] and if counsel does not ask, counsel cannot do that.

As such, in addition to the duty to advise clients about not intentionally destroying evidence, counsel is obligated to advise clients how to take reasonable precautions against accidental loss. Even though the standard for adverse inferences in both Alabama and the Eleventh Circuit is bad faith,[19] even an accidental or negligent loss of data can seriously impact a case in any number of ways. First, imagine the value of the client's case if counsel does not have the video file depicting the slip and fall, the cell phone pictures of the injury snapped while waiting for sutures, or the lack of any bruises or abrasions immediately after the incident giving rise to litigation. Sure, a witness can testify to these things, but it certainly may not be the same. Second, most cases do not have enough at stake to support or justify building a case for or against spoliation. Litigation is much more cost effective without having to undertake such additional efforts. Third, a finding of bad faith can occur more easily than one might think under certain circumstances.[20]

Counsel must be prepared to defend as reasonable the steps taken to preserve and collect relevant information. Never assume the client's IT personnel have the knowledge to adequately preserve and collect data without changes to the data. Inquire. Just like attorneys, who do not all practice in the same areas, IT personnel do not necessarily know all aspects of information technology. A database administrator is different from a network engineer, which may not have the same skills and knowledge as a helpdesk representative. Smaller companies have IT personnel that wear many hats (or contract out IT functions altogether) and may not necessarily know how to collect electronic data without altering metadata (which may later be deemed spoliation). If the client cannot adequately preserve and collect data without altering it, use a vendor to preserve and collect ESI.

Work with the client to identify who has control of relevant information and where the information is located. All employees of a client who control relevant information should be given instructions on what to preserve and how to preserve it. Identify third-parties who may have relevant information, too (more on that later). Finally, if the client is a company, remember the possibility of employees using personal devices (such as iPads, laptops, etc.) for work and therefore include such devices in the analysis of potential sources of data that must be preserved and searched because they are likely to be deemed to be within the "possession, custody, or control" of the client.[21]

A litigation hold notice must be circulated not just to players involved in events underlying the litigation, but potentially to several other people or departments. The notice should go to IT, human resources, the administrative assistants of custodians of information, potentially the immediate superiors of custodians, and anyone else who may have responsibility for repositories of relevant data. Always be mindful of the need to change or update a litigation hold as facts of the case change, new custodians are discovered, new data or types of data are found, and so on. Document who receives litigation holds, when the holds are acknowledged, when the recipients are reminded of the duty to preserve, and any further communication regarding preservation.

Always consider whether to send preservation demands to opposing counsel and/or to third-parties. Again, the individual case may or not require it, and counsel may have tactical considerations as to whether to send a written preservation demand. However, counsel should always consider whether a preservation demand is needed. When drafting the language, scope, and preservation steps requested, counsel must always assume that the same letter may be received back from its recipient asking counsel's client to undertake the same steps requested. That being said, it is possible that what is considered reasonable efforts for one party, or in one case, may differ for another. Specify, to the degree evidence is known, what that evidence is that must be preserved.[22]

Collecting ESI

While not every case will support the cost of forensic collection from all of the devices involved, and a less expensive method of collection may be justifiable, fabricated and altered electronic evidence, or selectively produced evidence, can be difficult to identify if not collected correctly. Fabricating emails, Twitter messages, etc., is simple,[23] and can be hard to identify if handled as PDFs. If the argument can be made that forensic techniques should be required in collecting evidence, then doing so is the safer course.[24] As in other contexts, however, counsel must be prepared for the same demand to be made to their client in discovery, so a factor to consider in whether to demand forensic collection of ESI is whether counsel's client can afford to produce in the same manner.

A Word About Metadata

"Metadata" is information generated by computer devices regarding the systems and files used. Metadata receives tremendous attention in electronic discovery and is one of the reasons that drives lawyers to (supposedly) "avoid electronic discovery." However, metadata does not always (and, indeed, rarely) has evidentiary value that is essential to a case. Most of the time, metadata is used in large document cases to assist in the identification, search, collection, and analysis of relevant ESI. When relevant documents number in the thousands, tens of thousands, or more, being able to search and analyze via metadata is essential to thorough, efficient, and cost effective representation, and counsel should consider collecting metadata, requesting metadata, or both.

In cases small enough to simply review documents, one after the other, start to finish, the analytical need for metadata is much less. In such cases, the primary value of metadata is from an evidentiary standpoint,[25] but is not necessary in every case. Metadata can be useful in determining such things as when a document was created or modified, the device from which it originated, and so on.[26] Metadata relating to pictures can identify the date, time, location, and device with which they were taken.[27] The usefulness of such metadata for authentication, factual investigation, and maintaining data security should be readily apparent. In many instances, such evidence can be admitted by a witness with knowledge, but in disputes as to when someone received a document, which version of a document existed when, whether a person had

received a particular document, etc., this information, coupled with hash values[28] can be invaluable.[29] This is particularly true in matching emails to their attachments.

If such issues are not involved in the case, and the number of relevant documents is small enough that metadata is not needed in order to search and analyze documents, then the value of metadata in a case is generally low.[30] However, metadata should generally be preserved, unchanged, at least initially, until the litigants can determine whether any issues exist requiring the use of metadata or until protocols or stipulations can be reached in the case.

Many do not realize that metadata is easily changed. Using the common "drag and drop" method of preserving documents by clicking on the file and dragging it to another folder or drive typically changes several items of metadata. Opening a file can change the metadata. If accurate metadata is going to be needed (or requested) in a case, consider employing technical assistance in preserving and collecting relevant ESI so that metadata is not changed (and, therefore, spoliated). Simply forwarding email to counsel can present similar problems as opposed to harvesting the emails from the computer on which they reside in the usual course of business.

Form of Production

Litigants can avoid receiving PDFs that are several thousand pages long as discovery responses. When drafting discovery requests, always consider the form of production. Both state and federal rules allow the requesting party to specify the form of production.[31] It is recommended to do so, even if only for certain types of data. Otherwise, parties have little control over the form in which they receive documents, which can be problematic and expensive for the requesting party due to inefficient search and review for documents (i.e., receiving a single 6,000 page PDF as a discovery response). Obtaining documents in a searchable format allows the attorneys and staff to more efficiently work with the file and leads to more effective analysis of the documents (and, in turn, the case).

That being said, some institutional clients refuse to produce documents in native format, and it is usually difficult to justify a refusal to produce native format documents if that party's request for production demands them. Discuss the form of production to be used in the case with the client before agreeing to a particular format with opposing counsel. Reversing an agreement can be difficult. However, if the case has even the *potential* to involve more than a couple thousand documents, either request them in native format or as static images (TIFF or PDF) with a word index and a metadata "load file".[32] Simply applying optical character recognition ("OCR")[33] to the documents is not nearly as helpful and can change the text of the documents. Native documents can be more problematic to work with, but are sometimes required, and almost always provide better information and analysis than other forms of production. In most cases, PDF format is easier to deal with, but request along with it an index of all the words in the documents and a load file. Failing to request this format at the outset risks the production of an unmanageable number of PDFs, making the case much more difficult and expensive to work on if there is no index built from the documents. Counsel should avoid getting stuck with more PDFs than the client will want to pay counsel to click through (or have the staff click through) to find particular documents. Obviously, scanned images of hardcopy documents must be reviewed manually since no electronic format exists, and OCR may be of limited benefit, depending on the quality of the scanning.

Native format production in particular will need to have chain of custody documented. Request chain of custody documentation along with the production and continue documenting chain of custody upon receipt. For this reason, consider requesting that a native format production of any significant size go directly to a vendor rather than through counsel's office (so that counsel is not at risk of being in the chain of custody). Either way, use a chain of custody form to document who has had the documents and what was done with them during each person's custody.

Not all documents need to be requested in the same format, so, for example, emails and spreadsheets can be requested in native format, with other documents in PDF accompanied by a load file of relevant metadata fields.

If no form of production is specified, then the responding party can produce documents either in the form in which they are maintained or in any other form that is "reasonably usable."[34] The rules provide little guidance as to what constitutes a form that is "reasonably usable," but many cases have clearly stated that producing documents in a static form, such as PDF, without useful metadata, when such information is available to the producing party, is not a "reasonably usable" form,[35] nor is it considered to be in the form "as kept in the ordinarily course of business."[36] Remember that using OCR on static images can change the contents of the files, so only use OCR on a copy so that the original text is maintained. If no form of production was specified or if the responding party intends to object to the form requested, then the responding party must notify the requesting party as to the form in which it will respond.[37] Such notification should be made in advance of the production—otherwise, the responding party runs the

risk of producing the ESI a second time in an acceptable format, notwithstanding *Ala. R. Civ. P. 34(b)(ii)*.[38]

Finally, Rule 45(c), regarding steps to protect the recipients of non-party subpoenas, was amended in 2010 when Alabama adopted rules regarding electronic discovery. Subpoena forms that predate those amendments should be revisited. Form 51A, in the Alabama Rules of Civil Procedure, is compliant with the 2010 amendments.

The Rules are Helpful in Smaller Cases

The Alabama Rules of Civil Procedure contain many provisions that are helpful in litigating smaller cases. First, discovery is subject to a proportionality analysis, as measured by such factors as the size of the case, the amount at stake, the importance of the issues, and the parties' resources.[39] In federal court, when an attorney signs a discovery request, the attorney certifies that the discovery requests are proportionally reasonable for the case. Accordingly, the scope of discovery in a case is subject to a determination of what is reasonable.[40]

Though the Alabama Rules of Civil Procedure do not expressly contain an equivalent to *Fed.R.Civ.P. 26(g)*, a similar requirement is implied.[41] First, under Rule 26(b)(2)(B), discovery requests can be limited based upon what is proportional to the case, i.e., what is reasonable under the circumstances. Second, though technically within the scope of discovery, some sources of data may be deemed "not reasonably accessible" and need not be produced absent a showing of good cause.[42] In determining whether the data source is indeed "not reasonably accessible," a proportionality analysis is required.[43] That is, certain data may not need to be produced based upon the factors set out in 26(b).

Though largely without substantive effect, Rule 1(c) also should be considered in determining the scope of acceptable discovery.

Now what do we do with it?

The ultimate goal of obtaining ESI is to admit relevant and helpful evidence at trial or in a dispositive motion (even if that preparation is intended to show that the case should be settled). Unless counsel's practice includes criminal law, "chain of custody" may not be a common term for counsel, but it should be with regard to ESI. Because it is recognized that ESI is fragile and easily modified, authentication requires some showing that the ESI is substantially the same as when it was obtained. This requires thought from the very beginning of the case, especially because failure to properly preserve and collect ESI could lead to problems with authentication at trial or summary judgment. During preservation and collection, consideration needs to be given to how ESI will be authenticated (and how the opposing party will authenticate its own ESI). Even if the case is being prepared for a summary disposition, ESI used to support or oppose the motion should be properly authenticated.[44]

Authorship once again becomes an issue with authentication in the context of ESI.[45] Even if it can be established, through metadata or otherwise, the computer on or from which ESI originated, authentication may require some evidence of whose fingers were on the keyboard.[46] Authentication must not always be established through high tech methods. After all, a handwriting expert is not always needed to admit documents. Probably the most common method is still through a witness with knowledge. But other common methods include unique characteristics, references to other communications or documents, etc.[47] Counsel should also consider stipulations (since it is very possible that both parties may face problems with authentication), requests for admissions, or through a more technologically sound method, such as through the use of hash values.[48] ESI can also be authenticated through proper chain of custody or through forensic techniques.[49]

A Word About Cooperation

Attempt to cooperate with other parties on discovery issues, because a lack of cooperation can lead to unguided, pro hac electronic discovery, which can take over the litigation and kill a client's budget. Cooperating with opposing counsel regarding scope of preservation, scope of production, form of production, tiered production, etc., can save tremendous amounts of time and money. Furthermore, it sets up discovery disputes in counsel's favor when counsel has attempted to address issues in advance and the opposing party refuses. A large factor in managing the case to lower costs is cooperating with opposing counsel in an effort to reduce the number of documents that must be reviewed by counsel.

More than one judge has stated that he/she has not had disputes come up when they were discussed by the parties at the outset. Even in state court, a meet and confer request should be considered if the potential for substantial issues regarding electronically stored information are recognized. Pointing out in advance to the opposing party the volume of data that its requests are likely to generate (and the expense associated with sifting through it) often makes the opposing party more reasonable in discussions of the scope of preservation and discovery. Furthermore, attempting to cooperate should be a first step in arguing for cost shifting in overly broad, burdensome discovery requests. While some clients are reticent to cooperate on such procedural matters,

buy in is often possible by explaining the potential cost savings, even if only to free up money in the litigation budget for a more vigorous defense on the substantive issues in the case. If need be, make the case for cooperation by showing the client that it can be strategic.

Whether to Engage an E-Discovery Vendor

The key to holding down costs in smaller cases is in the way it is managed, not necessarily in avoiding the use of a vendor, and the single biggest opportunity to manage costs is by reducing the number of documents counsel (or contract lawyers) must review. Consider using a vendor to host and provide review capabilities for discovery documents. While engaging a vendor involves cost on the front end, it is often cost effective for the client in the long run because managing thousands of discovery documents becomes easier and more efficient—it decreases the amount of time spent searching through PDFs or binders looking for documents as the case is handled. If the case involves more than a few thousand pages, discovery documents need to go to a hosting vendor so that better search and analysis of the documents leads to less time wasted manually searching in linear fashion for particular documents. If need be, review a sample of the documents in question (whether from what the client produced or what another party produced) to determine how long a review of the entire document set will take so that a comparison with vendor budgets can measure any savings resulting from a more efficient document review.

Document All Decisions

If a challenge is made to any decision made during discovery, whether concerning preservation, collection, production, or whatever, it is likely to be long after the decision was made. Accordingly, decisions regarding documents to preserve or not preserve, steps necessary to preserve, etc., and the reasons for such decisions, should be documented so that later scrutiny is conducted in light of the facts and circumstances as they existed at the time rather than in hindsight. For example, the decision not to preserve any emails of a given custodian is easier to defend as reasonable if it is recorded that the decision was a result of the fact that no email to or from that person was found among the emails of the key players in the dispute, even though some connection of that witness to the dispute was later discovered. Keep detailed records of who conducts searches, how those searches are conducted, how documents are preserved, who formulates keyword lists, how documents are collected, and so on. The standard is "reasonable inquiry," not "perfect inquiry," but unless those details are known in the face of a challenge when previously undiscovered documents emerge, showing that the newly discovered documents were missed notwithstanding a "reasonable inquiry" will be difficult.

Continue Conducting E-Discovery, But Do It Correctly

The overwhelming majority of evidence is on a computer device. While counsel must still inquire as to hardcopy documents, they are becoming fewer and fewer. Because most potentially relevant evidence is ESI, counsel's efforts constitute electronic discovery. Once counsel realizes that it is all electronic discovery now (and it is not going away), it is easy to accept that it must be conducted proficiently. As the amount of data involved in litigation increases (and it will), techniques to manage the data correctly, from the start of the case and throughout the discovery process, must be applied, whether by counsel or by engaged vendors. Failure to do so is risky and expensive.[50] Now that counsel realizes that she has already been engaged in electronic discovery, counsel should sit up and do so with confidence rather than be the shaky, wobbly new rider.

J. Paul Zimmerman, partner with **Christian & Small**, has an extensive litigation practice, leads the firm's Electronic Discovery practice and is on the Technology Committee. He often handles litigation involving product liability, trade secrets, covenants not to compete, and business litigation. A member of the Sedona Conference Working Groups 1 and 11, and Chair of the Claims and Litigation Management Alliance's eDiscovery and ESI Committee, Paul devotes much of his practice to defending companies facing cyber and data breach liability. He is a frequent lecturer regarding eDiscovery and is a graduate of the University of Alabama School of Law.

---

[1] *The Sedona Conference Glossary (4th ed.)* ("Electronic Discovery ('E-Discovery'): The process of identifying, preserving, collecting, preparing, reviewing, and producing electronically stored information ('ESI') in the context of the legal process")(" ESI: As referenced in the United States Federal Rules of Civil Procedure, information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper)").

[2] First, Alabama Rule of Professional Conduct 1.1 requires counsel to have, obtain, or associate counsel with competence in the necessary skills. Second, *Fed.R.Civ.P. 26(g)* requires a "reasonable inquiry" with regard to disclosures and discovery responses. It can be argued that the Alabama Rules of Civil Procedure impose a similar standard. *See n. xli.*

[3] *The Sedona Conference Glossary (4th ed.).*

[4] *See, e.g., The Sedona Conference, "Jumpstart Outline: Questions to Ask Your Client and Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production" (March 2011).*

[5] *See Sample Order of Judge Robert Vance, 10th Judicial Circuit of Alabama, available at https://thesedonaconference.org/system/files/Jefferson%20County-ESI%20Discovery%20Order.pdf (last visited 03/29/2015).*

[6] *See Motions for Sanctions Based Upon Spoliation of Evidence in Civil Cases, Report to*

the Judicial Conference Advisory Committee on Civil Rules (Federal Judicial Center 2011), available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/DallasMiniConf_Empirical_Data/Federal%20Judicial%20Center.pdf (last visited on 02/17/2015). While the data in the report is dated, it is the latest available information containing that level of analysis found by the author.

[7] *See Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522-23 (D. Md. 2010).

[8] "'The preservation obligation runs first to counsel, who has a duty to advise his client of the type of information potentially relevant in the lawsuit and of the necessity of preventing its destruction." *Point Blank Solutions, Inc. v. Toyobo Am., Inc.*, 2011 U.S. Dist. LEXIS 42239, *39, 2011 WL 1456029 (S.D. Fla. Apr. 5, 2011).

[9] *See Victor Stanley*, 269 F.R.D. at 521.

[10] *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 612-13 (S.D. Tex. 2010).

[11] *See Victor Stanley*, 269 F.R.D. at 522.

[12] *See EEOC v. New Breed Logistics*, 2012 U.S. Dist. LEXIS, *17-18 2012 WL 4361449 (W.D. Tenn. Sept. 25, 2012) (collecting authorities).

[13] *See, e.g., Point Blank Solutions, Inc. v. Toyobo Am., Inc.*, 2011 U.S. Dist. LEXIS 42239 *37 (S.D. Fla., Apr. 5, 2011).

[14] *Supra, note xiii.*

[15] *See, e.g., Ala.R.Civ.P. 37 (Committee Comments to Adoption of Rule 37(g) Effective Feb. 1, 2010)*("This rule is procedural and does not address the issue of whether and such a duty [to preserve] exists. However, when it does exist, the party must act appropriately, which may include issuing a 'litigation hold.'" (emphasis added).

[16] *See Best Practices in E-Discovery in New York State and Federal Courts, Version 2.0. Report of the E-Discovery Committee of the Commercial and Federal Litigation Section of the New York State Bar, Dec. 2012.* http://www.nysba.org/workarea/DownloadAsset.aspx?id=523 (last viewed 04/02/2015).

[17] "Good faith may require a party to take steps to alter the routine operation of the computer system or otherwise preserve appropriate ESI if a duty to preserve exists." *Ala.R.Civ.P. 37, Committee Comments to Adoption of Rule 37(g), Effective Feb. 1, 2010.*

[18] *See, e.g., Swofford v. Eslinger*, 671 F.Supp.2d 1274, 1281 (M.D. Fla. 2009)(sanctioning the sheriff's department counsel for spoliation for failing to properly circulate and monitor the client's preservation efforts).

[19] *Bashir v. Amtrak*, 119 F.3d 929, 931 (11th Cir. 1997). *Cf. Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F.Supp.2d 1317 (S.D. Fla.)(finding that the defendant negligently spoliated emails, but because negligence does not amount to bad faith, refusing to impose sanctions).

[20] "The court finds appropriate the imposition of fees and costs against [counsel] in light of his complete failure to fulfill his duty, both in his official capacity as General Counsel for the [sheriff's office] and as initial counsel for all Defendants in this case, to take affirmative steps to monitor compliance so that all relevant, discoverable information is identified, retained and produced." *Swofford*, 671 F.Supp.2d at 1287-88.

[21] *See Selectica, Inc. v. Novatus, Inc.*, 2015 U.S. Dist. LEXIS 30460, *9-10 (M.D. Fla. Mar. 12, 2015)("This court agrees with those courts that have employed the practical ability test to determine whether a party has control, and therefore a duty to preserve information…The employer-employee relationship is one that may result in an employer party having the necessary control over information in the possession of a non-party employee.")(numerous citations omitted).

[22] *See, e.g., Swofford*, 671 F.Supp.2d 1274.

[23] Several websites exist that allow the user to create a static image of fake social media messages. *Go to, e.g., http://simitator.com/generator/twitter/tweet; http://fakeconvos.com/.*

[24] "Lawyers can expect to encounter judges in both camps [regarding the rigors of authenticating computer records], and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Furthermore, although 'it may be better to be lucky than good,' as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you." *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534, 559 (D. Md. 2007)(Grimm, Paul J., M.J.).

[25] *ee Lorraine*, 241 F.R.D. 534, 547-48.

[26] *Id.*

[27] *United States v. Post*, 997 F.Supp.2d 602, 603 (S.D. Tex. 2014).

[28] "A mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified." *The Sedona Conference Glossary: E-Discovery and Digital Information Management" (4th ed. 2014)("hash coding").*

[29] *See Lorraine, 241 F.R.D. at 546-48.*

[30] The decision is often driven by a determination of return on investment—whether a review of the documents by counsel is cheaper than engaging a vendor to help reduce the number of documents to review. Generally, the most expensive aspect of discovery of electronic documents is the review by attorneys. Therefore, if the cost of engaging a vendor reduces the number of documents to be reviewed by attorneys enough that the cost of the vendor is offset by savings in the attorney's review time, then the vendor should generally be engaged. Also, when a vendor is engaged, the collection and production is often more defensible and the case can be handled more efficiently throughout the litigation, especially when factoring in the time needed for reviewing documents for motion proceedings, depositions, and trial preparation, using the vendor's analytical capabilities.

[31] *Ala.R.Civ.P. 34(b); Fed.R.Civ.P. 34(b)(1)(c).*

[32] A "load file" is created by a party or its vendor, and contains certain metadata fields that were requested or agreed upon. Common metadata fields produced in a load file include author, custodian, date created, date modified, date accessed, pathname, hash value, etc., that assist in the analysis and authentication of the documents.

[33] OCR allows a computer to recognize the words in a PDF as text rather than as an image.

[34] *Ala.R.Civ.P. 34(b); Fed.R.Civ.P. 34(b)(2)(D).*

[35] *FDIC v. Bowden*, 2014 U.S. Dist. LEXIS 77890, *38, 2014 WL 2548137 (S.D. Ga. June 6, 2014) (citing Advisory Committee Note to 2006 Amendments to Fed.R.Civ.P. 34(b)).

[36] *Teldyne Instruments, Inc. v. Cairns*, 2013 U.S. Dist. LEXIS 153497 (M.D. Fla. Oct. 25, 2013)(*citing Bray & Gillespie Mgmt., LLC v. Lexington Ins. Co.*, 259 F.R.D. 568, 585 (M.D. Fla. 2009)).

[37] *Ala.R.Civ.P. 34(b); Fed.R.Civ.P. 34(b)(2)(D). See also Aquilar v. Immigrations and Customs Enforcement Div. of U.S. Dept. of Homeland Security*, 255 F.R.D. 350 (S.D.N.Y. 2008).

[38] "The responding party's designation of form in which it will produce ESI should precede the production of ESI. Otherwise, the responding party runs the risk it may later be required to produce ESI in a proper form." Committee Comments to Amendment to Rule 34 Effective Feb. 1, 2010.

[39] *Ala. R. Civ. P. 26(b)(2)(B); Fed. R. Civ. P. 26(b)(2)(c).*

[40] *See Fed. R. Civ. P. 26(g).*

[41] *See Ala.R.Civ.P. 11(a)* ("...to the best of the attorney's knowledge, information, and belief there is good ground to support [the pleading, motion, or other paper];" Ala.R.Civ.P. 26 (Committee Comments to Amendment to Rule 26 Effective Feb. 1, 2010)("ESI is not reasonably accessible if its production from the identified source should be unduly burdensome and costly. The responding party must act in good faith under Rule 11 in so designating a source of ESI.")).

[42] *Ala.R.Civ.P. 26(b)(2)(A); Fed.R.Civ.P. 26(b)(2)(B).*

[43] *Bowden*, 2014 U.S. Dist. LEXIS 77890, 2014 WL 2548137.

[44] *See Lorraine*, 241 F.R.D. 534 (*sua sponte* striking all emails and other documents attached to the parties' cross motions for summary judgment, and giving leave to refile, because the exhibits were not properly authenticated).

[45] *ee, e.g., Commonwealth v. Koch*, 106 A. 3d 705 (Pa. 2014); *Smith v. State*, 136 So.3d 424 (Miss. 2014); *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012).

[46] *See* Grimm, Paul W., *Authentication of Social Media Evidence*, 36 Amer. J. Trial Ad. 433 (2013).

[47] *See Lorraine, 341 F.R.D. 534; note xlvi, supra.*

[48] *Id.*

[49] *Id.*

[50] *See Martin v. Northwestern Mut. Life Ins. Co.*, 2006 WL 148991 (M.D. Fla. Jan. 19, 2006).