Technology: E-Discovery Under Rule 26

Published 3/16/2013 in The Oklahoma Bar Journal, Vol. 84, No. 8

By Cody Cooper

Cody J. Cooper

Under Rule 26(f) of the Federal Rules of Civil Procedure (FRCP), opposing parties must now discuss e-discovery at least 21 days before a scheduling conference is heard or a scheduling order is due under Rule 16.1 Rule 26(f) also applies to "all sorts of discoverable information, but can be particularly important with regard to electronically stored information."2 This varies greatly from the current Oklahoma requirement under 3226(f), which states that "[a]t any time after commencement of an action, the court may direct the attorneys for the parties to appear for a conference on the subject of discovery."3 While Oklahoma statutes state that a discovery conference is discretionary, it is mandatory under the federal rules. Additionally, both sides are required to discuss the form or forms in which discovery will take place, what information will be within the scope of the suit, issues

about claims of privilege, and e-discovery.

The advisory committee notes for the 2006 amendment to FRCP 26 state, "[w]hen a case involves discovery of electronically stored information, the issues to be addressed during the Rule 26(f) conference depend on the nature and extent of the contemplated discovery and of the parties' information systems. It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful."5 The practical implications of this note are clear. The committee expects both sides' counsel to cooperate with each other and have a full understanding of their respective client's data when they go to the conference.

As the advisory committee notes make clear, it is each attorney's job to become familiar with their client's information systems. Indeed, in the discovery conference, counsel is often required to exercise this working knowledge by discussing what data is in each system and the respective retention policy for that system. This means that counsel must become intimately familiar with a client's data creation and storage and be able to be conversant in the same. This could require looking at a map of each client's database for his or her company or going through each application your client is using and discussing where the data is stored for each application.

Furthermore, the volume and dynamic nature of electronically stored information may further complicate preservation obligations. "The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases

uncertainty and raises a risk of disputes."6 Again, this means that attorneys must be forthright in the information they possess, and both sides need to cooperate in the discovery conference or risk potential adverse actions (sanctions, etc.). The discussion between attorneys needs to be open and honest, and both sides need to focus on "the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities."7

Additionally, courts should be hesitant to provide one side an overly burdensome or broad preservation order for fear that "[a] blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations."8 In fact, the advisory committee for the Federal Rules of Civil Procedure states that "[a] preservation order entered over objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances."9 Ultimately, the parties need to take all of these considerations into account and try to reach a reasonable agreement.

ESI AND E-DISCOVERY

Before delving into a brief overview of what I believe are some of the most important aspects of e-discovery, remember that parties to litigation can always agree to produce discovery in paper format, not electronic. However, this doesn't mean you can avoid electronic discovery (e-discovery). As any attorney knows, discovery is a critical process of litigation that is often tedious, time-consuming and incredibly expensive. While traditional document discovery requires combing through thousands upon thousands of pages of paper (many times much more), e-discovery could exponentially increase that amount to stratospheric numbers in the millions, tens of millions, or even hundreds of millions. Breaking it down to its most rudimentary thought, e-discovery is simply the discovery of electronically stored information. While

seemingly simple, the actual process of e-discovery, as well as the potential adverse effects, is far from it.

For as long as computers have been around, data has been stored. Whether in the form of a paper punch card, a floppy disk, a zip disk, a hard drive, or in the ever-present cloud, people have been storing computer-generated data. Since its invention, the entrepreneurial race has been creating larger and faster electronic storage in paradoxically smaller packages. Some industry experts believe Moore's law equally applies to the development of electronic storage as it does to processors. Moore's law, in an over-simplified nutshell, is the idea that every 18 months the number of transistors on an integrated circuit doubles. This is thought to be equally true of the amount of storage space that can fit in an identical space, meaning more storage in a smaller area. With the exponential increase in storage availability comes a number of hidden costs and dangers, particularly when it comes to e-discovery.10

WHAT IS ESI?

ESI is an acronym used to describe "Electronically Stored Information." ESI encompasses all data that is stored electronically. I emphasize these words not for dramatic effect, but to call your attention to the broad scope of ESI. Say, for instance, you have a contract that your client and another party have signed. Clearly this physical paper copy isn't ESI. But, if you decide to scan that document and send it to yourself in an email, voilà, you've got ESI. Some of the types of ESI most people are probably aware of are application data (Word documents, Excel sheets, PowerPoint projects), messaging systems (emails, instant messages, voice mail, electronic calendaring) and databases. But ESI also includes things that you might not be aware of. For example, your computer and most applications generate data every time you perform an action like clicking on specific data, making

revisions to a document, searching for a specific website, watching a YouTube video or listening to a song. These examples, however, are far from an exhaustive list. Since attorneys are responsible for producing and requesting discovery, it is critical that any attorney dealing with e-discovery have a general knowledge of the types of information that could potentially be subject to discovery.

It is equally important that attorneys have a working understanding of the types of electronic information you might want to request or you may need to produce because of the possible ramifications for failing to do so. Your clients will rely on you to know what to request, and it is incumbent on each attorney to recognize the different types of data to adequately draft and respond to discovery.

Now that we have a working understanding of what ESI is, we need to look at one of the most important things about ESI and that is how ESI is stored. Other than knowing what ESI to look for, the second most important thing an attorney needs to know is where to look for ESI. While ESI storage may seem common sense, it’s helpful, nonetheless, to provide a refresher (or introduction depending on the reader) to the places information can be stored.

There are three primary ways ESI can be stored: online, nearline, or offline.11 First, ESI can be stored online. This simply means that information is stored at a readily accessible location and requires no human intervention (think hard drive on your computer or a cloud accessible to anyone upon immediate request). Near-line storage can be summed up as direct access removable storage (think flash drives, portable hard drives or CDs/DVDs). Offline storage is most commonly backup tapes. These are just magnetic tapes, similar to cassette tapes, or for those of you young enough to have no idea what a cassette tape is, just imagine a spool of plastic ribbon encased in a plastic casing that is capable of storing information on it. Storage location can be incredibly

important because, while producing data from readily accessible records like the hard drive from a computer or a USB drive is relatively simple, the costs and difficulty can potentially increase exponentially when backup tapes are involved. The difficulty can increase because of the amount of information that can be stored on backup tapes. Because the information is historical, those working with it are likely unfamiliar with what is stored on the tapes. This increase in costs can lead to fights between the sides as to who should bear the burden of producing the requested data.

PRESERVATION OF DATA

Aside from combing through the data you plan to produce or receive from the opposing side, preserving the right data and eventually producing it is likely the most onerous part of e-discovery. Preservation of data has many important questions that are too technical to be discussed in their entirety within this article, but this should provide a brief overview. However, it is important to recognize that there are many more complex questions that will arise throughout the ongoing preservation of data for purposes of litigation. The first thing to think about when you are faced with the question of preserving data for ongoing or pending litigation is, when does your obligation to preserve begin? Typically your obligation begins when you reasonably anticipate the evidence will be relevant to future litigation.12 If you are the requesting party, you can avoid a potential dispute as to when your opponent should have anticipated the data being relevant to litigation by drafting a litigation hold letter and sending it to your opponent. At its most rudimentary level, this letter tells your opponent the locations and types of data you might request so that they are put on notice to not destroy the information.13 Second, you should determine what is your client’s data retention policy? A retention policy is a set of official guidelines or rules governing storage and destruction of documents or ESI.14 In Arthur Anderson LLP v. United

States, the United States Supreme Court recognized there is nothing wrong with data retention policies that call for destruction of documents so long as the destruction does not occur at a time when a legal duty to preserve that evidence has arisen.15 The burden to preserve is not unilateral to defendants, "plaintiffs also have a duty to suspend regular destruction under records-retention policies once they plan to file suit."16 Understanding your client's data retention policy is important because it is the duty of each attorney to ensure that their client preserves all relevant data throughout litigation.

"The obligation to preserve evidence arises when a party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."17 The duty to preserve evidence is one that is placed on counsel.18 In addition to implementing a "litigation hold" on the destruction of relevant information, counsel is responsible for ensuring that a client actually does implement such hold and continues to implement the hold throughout litigation.19 "To do this, counsel must become fully familiar with the client's document retention policies, as well as the client's data retention architecture."20 This means that counsel is required to become intimately familiar with her client's data and procedures. After you have an understanding of what data your client has and their retention policy, it is counsel's responsibility to locate relevant data and ensure the client preserves that data. This means you have to preserve data that could potentially be subject to discovery, even if it is not specifically requested.21

PRODUCING AND REVIEWING DATA

Once data has been preserved, the big question then becomes how to review and eventually produce the data. Reviewing data for privilege presents a potentially massive undertaking for counsel, depending on the volume and sensitivity of the

information being produced. For particularly large cases, counsel will likely have to request large extensions in production deadlines and may even have to increase the number of attorneys reviewing the data. Parties have the ability to stipulate that any production of privileged data to the other is deemed to not be a waiver of any such privilege; but again, this topic is more detailed than this article intends to cover. Under the FRCP (Rule 34), the requesting party can request a specific format, and the producing party can respond by complying or objecting. But if they object, they must provide an alternative format.

The Oklahoma statutes, however, do not address production of data in specific formats, and the parties are left to decide and then ask the court to referee when they can't agree. Much of the data production argument will involve production in native or non-native format. Native format means the format in which the information is naturally kept. Native format is important because it contains metadata, which means that native format contains "hidden" information such as, among other things, who created the data, when the data was created, and what application created the data. Metadata can best be understood as "data about data" that can't be seen just by looking at an individual record. Think of it as looking in your iTunes music library at your favorite song: you can see the artist and album, but you can't see what year it was created or the producer of the music. Metadata would allow you to see those things. Producing documents with metadata also raises a number of issues.

When a party receives a request for electronic data, the party and counsel "are under a duty to make a reasonable search for all relevant, non-privileged documents and ESI within the scope of the particular request (assuming the request is well-framed)."22 Finding this data can present difficulty depending on the number of records available. Keyword searches are primarily how data is chosen, and they "work best when the

legal inquiry is focused on finding particular documents and when the use of language is relatively predictable."23 Fashioning too broad of a keyword search will likely result in a dispute between the parties as well as the potential to return significantly more documents than desired. Too narrow, and the potentially helpful documents could be left out. Too broad and a party could be buried in information. The difference between a good search and a bad search can be the difference of finding (or disclosing) the smoking gun and being lost in a forest of useless information.

POTENTIAL ADVERSE EFFECT

Under both FRCP 37 and 12 O.S. 3037, the court has broad discretion to punish parties for failing to comply with discovery. Default judgment or dismissal, sanctions, and adverse inferences are the primary concerns with failing to cooperate with e-discovery. In one of the five Zubulake cases, UBS failed to comply with preservation instructions and repeated orders by the court. The court then threatened them with an adverse inference at trial.24 The court followed through with its threat and permitted the jury to make an adverse inference with respect to emails deleted and irretrievably lost when UBS's backup tapes were recycled.25 In the end, the Zubulake jury rendered a judgment against UBS for more than $29 million.26 In Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc., a Florida court issued an adverse inference against Morgan Stanley for "overwriting emails, failing to timely process hundreds of backup tapes, and failing to produce relevant emails and their attachments."27 Morgan Stanley had judgment entered against it for $1.45 billion based largely on the instruction given, but that judgment was subsequently successfully appealed.28

These two cases are a subset of cases imposing harsh penalties on parties that purposefully fail to comply with courts and opposing counsel during e-discovery. Sometimes there is little

an attorney can do to ensure a client complies with what is expected of them, but it is important that counsel communicate the potential weighty risks a client, and their counsel, could be faced with in the event that they aren't complicit.

CONCLUSION

E-discovery is an ever-increasing and necessary part of litigation. Society's increasing reliance upon computers for both personal and business activities means that electronic data will continue to increase every day. This presents a challenging problem for lawyers and their clients. While this mountain of data can be used both as a sword and as a shield, even the most experienced lawyer needs to tread the waters carefully. It is important to keep in mind your ethical obligations to your clients, courts and opposing parties, and focus on a fair and reasonable resolution for all discovery disputes. Depending on the nature of your case, often times it is cheaper to agree with opposing counsel to simply conduct discovery in paper form rather than incurring the excess expense of producing massive amounts of data; but regardless, you will likely be required to deal with esi and e-discovery in some form or fashion. Ultimately, this decision will have to be something each attorney will decide based on their belief of what is best for their client.

Cody J. Cooper is an attorney in the Litigation Department of Phillips Murrah P.C. His primary practice areas are commercial litigation, class actions, complex torts and intellectual property. A Norman native, he graduated with honors from OU College of Law in 2012 and received his bachelor's degree in management information systems and finance. He served as the managing editor of the OU American Indian Law Review.

FOOTNOTES

1. Fed. R. Civ. P. 26(f) (2012).
2. Fed. R. Civ. P. 26(f) (2006 committee notes).

3. 12 O.S. 3236(f) (2012).
4. Fed. R. Civ. P. 26(f) (2006 committee notes).
5. Id.
6. Id.
7. Id.
8. Id.
9. Id.
10. Much of this paper is derived from secondary sources discussing e-discovery and its seminal cases. With that said, any attorney looking to educate themselves on e-discovery and digital evidence would be best served by obtaining a copy of West's Nutshell Series for Electronic Discovery and Digital Evidence written by Shira A. Scheindlin and Daniel J. Carpa. The commentary for the 2006 amendments to the Federal Rules of Civil Procedure is also helpful when reviewing Rule 26(f).
11. Shira A. Scheindlin & Daniel J. Capra, Electronic Discovery and Digital Evidence 14-16 (West 2009).
12. See Andrew R. Lee, Keep or Toss? Document Retention Policies in the Digital Era, 55 La. B.J. 240, 244 (2008).
13. See generally Bradley C. Nahrstadt, What's the Deal with Litigation Hold Letters? (With Forms): Hold on a minute: How do these things really work?, 18 No. 6 Prac. Litigator 23 (2007); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).
14. Id. at 33.
15. See Arthur Anderson LLP v. United States, 544 U.S. 696, 704 (2005).
16. Scheindlin & Capra, supra note 11, at 35.
17. Id. at 36.
18. Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-32 (S.D.N.Y. 2004).
19. See id. at 432.
20. Id.
21. Lee, Supra Note 3, at 240.

22. Scheindlin & Capra, supra note 11, at 137.
23. Id. at 137-38.
24. See generally Zubulake, 229 F.R.D. 422.
25. Id. at 437.
26. Nahrstadt, 18 No. 6 Prac. Litigator at 24.
27. Id. at 25
28. Id.