Making Sense of E-Discovery: 10 Plain Steps for Producing ESI

The following article provides a practical guide to producing electronically stored information (ESI) that lawyers can apply immediately in their practices. The author has divided the full article into two parts to cover five steps in each section. Part 1 focuses on the initial investigation that lawyers can undertake in order to be fully prepared for the "meet and confer" with opposing counsel.

Have you ever been handed a detailed flowchart on ESI and wondered what to make of it? Have you read case law summaries about ESI and thought, "how do I actually apply this holding to my practice?" And when you do produce ESI, is there any concern whether the methods you used would pass muster if critiqued by a federal judge?

When the next big case comes in, have a plan to make sure you do everything right. Of course, you'll have to tailor your methods and budget to the size of the case, but at least some ESI will come into play any time communications or stored data might become evidence. If producing ESI takes you out of your comfort zone, here are 10 plain steps that might work for you.

1. **Prepare Your Team.** As soon as you staff the case within your office, hold a team meeting to discuss the nature of the case and what kinds of ESI might be relevant to prove the claims and defenses. Be sure to include everyone at the meeting, for example a shareholder, an associate and a paralegal. In discussing ESI, consider not just computers, but other things like workplace video cameras, parking garage entry logs, and other records kept electronically. You should stress the importance of keeping a journal at your law office to track all the decisions you make regarding ESI. The journal needs to be easily accessible by everyone on your team and should be updated regularly. In fact, the minutes from your meeting should be the first entry on the ESI journal. You may also want to review social media and run Google searches on anyone who is likely to be deposed, and print everything immediately in case it becomes unavailable later. You should also be sure a spoliation notice is mailed to opposing counsel and a preservation letter or "litigation hold" letter goes to the client. Make them short and understandable, with possible inclusion of social networking sites as part of the litigation hold.

2. **Meet With the Client.** Set up a conference at your client's office to review its organizational chart and discuss how information is stored electronically among various people and locations. In attendance for the client should be a decision maker, the person most familiar with the issues in the litigation, and a member of the information technology (IT) department who knows how much work goes into collecting data. Keep in mind that the IT person may be more optimistic at this meeting in front of his boss than he might be when you talk to him on the phone in private. From your law firm, bring the whole team from your initial meeting and perhaps also someone from your IT department who can ask some of the technical questions. Keep in mind that typically the producing party pays for ESI,

and though your client may be weighing the cost of being thorough against the risk of sanctions, you are ethically required not to let the client cut corners. Explain to the client what the rules of civil procedure require, and note that you can save costs by working with opposing counsel to limit the scope of the search. Record everything in your journal, and be sure the client has properly implemented the litigation hold in all relevant departments and among all information systems. You might also go over the client's data retention policy to be sure it is simple, enforceable, and actually being enforced.

3. **Interview the Employees.** In meeting with the client you probably learned the names of most of the employees who might have information relevant to the case. You should interview all of them and find out how many devices they use in performing job duties, including, for example, e-mail, instant messaging, home computers, voicemail, text, cloud storage, social media, special software programs, and perhaps log books where other data is recorded. If they are heavy users of online networking, you might advise them not to make statements online that could impact the case, or else to increase their security settings. Anything they have accessed as part of the job is subject to being searched. This obviously raises privacy issues when employees use their personal e-mail accounts occasionally for business purposes. You should also find out if employees are new to the job, and if so, whether their predecessors may have some of the information. Take detailed notes for your journal and be sure the employees are properly observing the litigation hold implemented by the company. You have to be the watchdog because, although employees may seem helpful and willing, they might not try their hardest on completing tasks that don't fall within their job description. Make a checklist of all the sources of information they have identified and, for anything outside the company premises, write down how and when they plan to provide it to you. If one or more employees are no longer with the company, the IT department should be able to identify what data they had when employed, as well as anything they may have downloaded and taken with them.

4. **Outline the Plan.** Here you need to think mainly about three things: what ESI your client has, what issues are relevant to this particular lawsuit, and what your obligations are under the Federal Rules of Civil Procedure, the Federal Rules of Evidence, and/or state law. Generally speaking, FRCP 16 requires you to know how to produce ESI so that agreements can be made for scheduling orders. FRCP 26 requires discovery to be proportional to "the needs of the case" as measured by a cost-benefit analysis. It limits discovery of ESI from sources that are "not reasonably accessible," but of course your client cannot deliberately make its data "not reasonably accessible." It also tightens the definition of relevancy to the claims and defenses at issue and not simply to anything that "appears reasonably calculated to lead to" the discovery of admissible evidence. FRCP 33 specifically allows the production of ESI in response to interrogatories, and FRCP 34 explains how ESI should be produced in response to a document request. Often the requested form is native file because those files tend to reveal

the most, and you might not have the software necessary to view ESI in other forms. FRCP 37 allows judges to impose sanctions for discovery abuses, but includes a safe harbor for ESI that is no longer available through no fault of your own. FRCP 45 protects non-parties from some of the costs and burdens of e-discovery similar to the rules governing parties. FRE 502 protects attorney-client privileged communications and excuses inadvertent disclosures if you took reasonable steps to prevent the error and quickly attempted to remedy it. You may want to enter into a "clawback agreement" from the outset to give more reliability than Rule 502 which hinges on reasonableness and inadvertence. FRE 901 requires that evidence be authenticated to verify that it is what it claims to be, and metadata can be used in that respect for ESI. These federal rules have generally been incorporated into Florida Rules of Civil Procedure 1.200, 1.201, 1.280, 1.340, 1.350, 1.380 and 1.410, although there is no state "meet and confer" requirement. In reviewing these rules and outlining your discovery plan, you should name the custodians and ESI sources, noting what you believe would be unduly burdensome, not reasonably accessible, or otherwise limited by the proportionality rules. Indicate in your journal that you made this outline.

5. **Confer with Opposing Counsel.** Now you should be prepared to have a meaningful conference with opposing counsel regarding e-discovery. If this is a federal case, the conference under Rule 26(f) specifically requires discussion of issues about disclosure or discovery of ESI, including the form or forms in which it should be produced. The rule requires all parties to meet at least 21 days before a scheduling conference and requires that you make initial disclosures no more than 14 days after the meeting, unless an objection is made or another time is set by stipulation or court order. You will have to describe ESI by category and location in your initial disclosures, so if you have an objection to the time period, you should raise it at the conference. Discuss these issues with your IT professional and remember only to request from opposing counsel what you think you will need. Depending on the circumstances, you might propose the use of a court-appointed forensic examiner with both parties to split the cost. You might also suggest that the parties phase the discovery from one step to the next, for example limiting it to five custodians and 10 keywords, and then choosing the next step from what that search produces. Stipulated confidentiality orders may be appropriate. If the litigation is asymmetrical, typically where the defendant holds all the information and the plaintiff has virtually nothing, it may be more difficult to negotiate with opposing counsel because the cost and burden are not shared. However, as a practical matter, attorneys who file plaintiff's cases like this may not be focusing on ESI. Nevertheless, in e-discovery, your role as a zealous advocate does not mean you should make e-discovery overly difficult for opposing counsel. The members of the Sedona Conference published a "Cooperation Proclamation" in July 2008 that is meant to facilitate cooperative, collaborative and transparent discovery. The Sedona Conference is a group of jurists, attorneys, in-house counsel, government lawyers, and others who generally believe that discovery should be easier and less expensive,

because justice delayed can be justice denied. You can visit the website at www.thesedonaconference.org.

The following is a continuation of the article, *Making Sense of E-Discovery: 10 Plain Steps for Producing ESI*, which appeared in the March 2014 issue of *The Briefs*. Part 1 discussed the initial investigation that lawyers can undertake in order to be fully prepared for the "meet and confer" with opposing counsel. This Part 2 focuses on the actual process of collecting, filtering and searching the data in order to produce it.

6. **Collect the Data.** Collecting data is not the same as filtering or searching; here you are simply corralling all of the sources of ESI so that later they can be searched in their entirety. The key is to figure out where everything is located. For example, there may be servers in California holding data that one of the custodians inputs from time to time for a particular project involving the West Coast. If you are collecting old data, don't confuse the term "backup" with "archive." A typical backup application takes periodic images of active data, usually only for a few days or weeks, to provide a method of recovering records that have been deleted or destroyed, such as to facilitate a disaster recovery. An archive is designed to provide ongoing access to decades of business information. The collection of data should be fairly inexpensive, but communication is key. If a self-collection error is made, for instance by collecting in such a way that metadata is lost, the entire process will have to be restarted, which could be extremely expensive. One of the critical points in collecting data is to understand that this is your obligation as counsel; you cannot leave it entirely up to the client. Whether you use a vendor at this stage, later in the process, or not at all, depends largely on the size of the document request. If you ask detailed questions about pricing plans and "scalability" of the process, you might find an affordable option with a vendor. However, no matter who is going to collect the data, the attorney must actively assist in the process. Your goal is to collect the entire universe of data from the sources that you have identified within your client's network. Of course this raises concerns about personal information that may be captured as well. Be careful about taking physical items (e.g., thumb drives) and the chain of custody issues that follow. Naturally you want to lessen the chance of having to be called to the stand as a witness. When the process is complete, you should be able to check off every source from the outline you created, and ensure that each was captured in its entirety.

7. **Filter into Groups.** This stage is sometimes called "culling" or "processing," where you transfer all the collected data into a software program, such as Nuix or Symantec's Clearwell eDiscovery Platform, so that you can filter it by keyword, data range, or some other way. You are not yet reviewing the documents themselves, but only running data sets to see how many hits come back. Courts have rejected attorneys' requests for opposing parties to search the entire

universe of collected data prior to filtering. When you think you have the right filters in place, you will need to get written confirmation with opposing counsel that the data sets you intend to search are acceptable, because you do not want to have to search the same material twice. Programs should have "deduplication" capabilities to eliminate duplicates and near-duplicates from the data set. When you filter into groups and then see the number of hits, you will need to get a sense of how many documents might be generated by those hits. One megabyte of e-mail generally translates to around 60 pages of paper. Forty megabytes would be 2,400 pages, which is roughly one banker's box. One gigabyte is 1,024 megabytes, which translates to 61,440 pages, or almost 25 banker's boxes. There are a number of variables to these estimates, however, such as how many of the documents are e-mails versus word-processed documents, spreadsheets, presentations, PDF's, images, text files, or other types of files. For example, one megabyte of e-mail may be 60 pages, but one megabyte of spreadsheets may be 150 pages. Another issue to consider is whether any of the files have been compressed, such as in ZIP, RAR or other formats (some types of files compress more efficiently than others). Whereas one megabyte of text e-mail could be 60 pages, one megabyte of compressed e-mail could be hundreds more. You may want to consult with an expert at this point because the page estimates will be important for budgeting. The review costs for relevancy and privileges are usually driven by the quantity of page equivalents.

8. **Search for Relevancy.** Now that you have a finite number of documents to search, you have two choices: either perform a "linear review," which means going through them manually at your billable rate, or use technology assisted review (TAR) which will apply predictive coding to determine which documents are most likely to be relevant. You may notice that online retailers already use predictive coding to offer products you are likely to purchase, based on past sales. Statistics indicate that TAR is actually more accurate than human review, and in fact, some studies show that two attorneys who search the same data sets for relevancy end up with vastly different document productions. However, if a computer is going to search for relevancy, you will probably need a subject matter expert (SME) to provide the search strings, because a computer won't know the facts of the case or the applicable law. There is also the question of whether using one SME is enough, and whether the SME created the right search strings. Linear review theoretically avoids those issues, but clients who choose linear review may find more than 70% of their e-discovery legal fees are spent on this step (more than all others combined). As a practical matter, if there are hundreds of boxes of documents to review, any human being is going to have trouble focusing for days or weeks on end, and there is an argument to be made that someone with a law degree should not be doing that kind of work. The same is true for reviewing documents that have been produced to you by opposing parties. Again, an e-discovery vendor can explain more about the pros and cons as to your particular case. It may be worthwhile to speak to a few different vendors on the phone, as some have very different approaches, and the

material they post online can look like a physics report from NASA. Be sure to provide your client with enough information to make a reasoned decision, and confirm it in writing.

9. **Audit Your Results.** This is an important and often overlooked step, sometimes called "sampling" or "quality control sampling." It allows you to test a small random set of documents to make informed decisions about the entire production. After searching based on relevancy, whether by linear review or through TAR, you will be left with a responsive set and a non-responsive set. You need to randomly sample the non-responsive set and ensure they don't include anything relevant. Document your findings carefully in your journal. If you find relevant information in your non-responsive set, you obviously need to revisit the previous step, improve your approach, and run another audit. Since the relevancy search can be such an expensive endeavor, you should think very carefully from the start about how to catch every potentially relevant document and thereby avoid failing the audit. The ultimate goal is to be sure your ESI production is defensible in the court of law, and a number of legal opinions around the country indicate that sampling and other quality assurance techniques must be employed to provide reassurance to the court. The party selecting the methodology must be prepared to explain the rationale for the search method selected, demonstrate that it was appropriate for the task at hand, and show that it was properly implemented. Without an audit, you will never really know if all your hard work paid off.

10. **Review for Privileges.** The final step usually requires human review. When you look over your responsive set of documents and get ready to produce them, you need to review them for privileges. This is not as simple as it seems; you will need to know how the case developed through time, when the legal problems started to occur, who was dealing with those problems from which locations, and how the issues morphed into litigation. At a minimum you will need a complete list of in-house and outside counsel who were communicating with your client during the entire time period. You cannot simply look at the "To," "From" and "Cc:" lines on an e-mail, nor can you just search for attorney or law firm names, because you might find an e-mail from your client's CFO to the CEO stating, "I spoke with our Orlando counsel yesterday and they told me …." You should also consider the actual elements necessary to claim the attorney-client privilege, particularly in that the communication was for the purpose of securing legal advice, and consider whether it was waived by including outsiders on the communication or otherwise by disclosing it to others. If you pull every document between lawyer and client, such as "I'll meet you in the lobby of our building at 2 p.m.," your privilege log is going to be as thick as a dictionary. On the other hand, many lawyers will tell you that privileged documents are almost always inadvertently produced. As discussed above, there are clawback provisions in FRE 502 that can be incorporated into an order or court-approved agreement prior to the production. FRE 502 also limits a potential waiver to the particular issue that was the subject of the communication. When reviewing for privileges,

also consider the work product doctrine, which is owned by the attorney, as well as the joint defense privilege/common interest rule, and the accountant-client privilege under Florida law. You also need to be on the lookout for any potential trade secrets or other confidential business information that may be contained in the documents, but the older the documents are, the less likely they will divulge trade secrets. After you make your privilege log, Bates stamp the rest of the responsive set, and produce them as a proper, defensible production of ESI.