

# Electronic Evidence Best Practices

By Sharon D. Nelson and John W. Simek

© 2008 Sensei Enterprises, Inc.

By rights, anything entitled “Electronic Evidence Best Practices” should be the length of an epic novel. This is not a short subject and trying to address it concisely means, necessarily, that the subject is being given short shrift. Nonetheless, the effort is worthwhile because so many lawyers continue to flounder whenever they encounter electronic evidence. Bearing in mind that we are only hitting “the top of the waves,” the guidance that follows may be of assistance in formulating your plans when electronic evidence is in issue.

**Look at all data (your law firm data AND client data) as possible evidence.** Deal with litigation before it happens. What does this mean?

- Develop a document retention policy, assembling a team of inside and outside counsel, management, subject matter specialists (SOX, HIPAA), and IT folks to craft it.
- If you don’t need data, get rid of it. It’s just more chaff heading the wheat you may one day need.
- For the data you keep, make sure it is retained in such a manner that you can easily find and produce it if necessary.
- Ensure that you are in compliance with the law, federal and state regulations, your own policies and by-laws and industry standards.
- Enforce the policy, because it is useless if you do not.
- Review the policy at least annually, because technology morphs rapidly, laws and regulations are born more quickly than bacteria in a petri dish, and businesses themselves evolve and present new requirements.
- One of the very best resources for understanding records management is ARMA International, [www.arma.org](http://www.arma.org)

**STOP! STOP! STOP! When a litigation hold occurs, preserve the evidence.** For some reason, this rule is honored in the breach. Do not have a panic response to a litigation hold because you will very surely “put your foot in it.” When does a litigation hold take effect? A rough guideline is that a litigation hold takes place when a lawsuit or regulatory action has commenced or when you know or reasonably should have known that such action was likely. Is that a little dicey to implement? Absolutely. When some nutcase says “I’ll sue you!,” you are probably not in a litigation hold. But when, as an example, someone has written several letters and/or retained counsel and expressed a credible grievance, it is certainly time to make sure that you are abiding by the rules of litigation holds as articulated in *Zubulake v. UBS Warburg* and its brethren. Now that you know there is evidence to preserve, what do you do?

- Have a Litigation Hold Response Team in place. Pre-identifying the folks will make things happen faster. Your team should include inside and outside counsel,

management, IT folks and those who have specific knowledge of the facts at issue.

- If there are workstations that should be unplugged and taken out of commission (or you can use Norton Ghost to replicate the drive on a new drive and simply lock up the originals), do so.
- It is now time to cease defragging, disk optimization, deleting data, adding new programs, or doing anything that might overwrite relevant information.
- Do not “stomp on the evidence.” If you or client’s IT staff takes a look at the evidence to see “how much trouble we’re in,” you will be changing the dates of last access, at the very least. Relevant evidence should be preserved, not explored, at this point.
- Consider carefully where all the evidence is – and don’t forget the Palm Pilots, BlackBerrys, cell phones, voice mail, etc.
- Become familiar (and yes, this is now an attorney duty) with the backup system. Take your bottle of Advil with you, but sit down and talk to the IT staff until you understand the backup process. Case law is now mandating that attorneys understand their client’s backup system so they will understand what data is where and what steps must be taken to preserve evidence.
- Do you need to take backup media out of rotation to preserve it?
- If you have third party backup, they need to be notified of the duty to preserve.
- Look at your document retention policy and alter it as needed for the duration of the litigation hold.
- Write a memo to all those potentially involved, paying particular attention to the key players, spelling out the duties imposed by the litigation hold – and the fearsome potential consequences of spoliation, including huge fines, the inability to use some testimony, the requirement that you will have to pay for any remedial action, and, worst of all, the potential imposition of the dreaded adverse inference instruction.
- If you are instituting the litigation, make sure you write a clear preservation of evidence letter, identifying the issues, the people involved, and brandishing the sword of spoliation as a consequence of failing to comply.
- Do it again down the road. Case law now makes it clear that a single memo issued at the outset is insufficient. Lawyers, though not precisely expected to “babysit” their clients, are expected to monitor the litigation hold and to issue periodic reminders to make sure, insofar as they can, that it is complied with.

**Gather the evidence with painstaking care.** When you are responsible for finding the appropriate evidence in a case, you have a difficult duty. Most lawyers are not technologists, but the 21<sup>st</sup> century is now requiring that lawyers have at least a fundamental understanding of where electronic evidence may be, so that they can properly collect evidence in a case. Here are some tips:

- Get help. Someone who understands information technology will be invaluable. You may want to use someone from your own firm, if you have an IT department and you will surely want to use someone from your client’s IT department.

- Evidence tends not to be in a single place. Your client may have a headquarters, but do they have branch offices? Is backup or storage of data outsourced to third parties? Who hosts their website? Do employees have laptops? Cell phones? PDAs? Do they work at home on their own computers? Don't forget digital media cards, digital cameras, voice mail, etc.
- If you are crafting discovery, make sure all of the sources listed above are identified, as well as the names of the principals involved. The more you can identify the nature of the action and the folks likely to be involved, the more you have definitively placed the other side on notice about what must be preserved and produced.
- At all times during the gathering of evidence and the computer forensics process, make sure a proper chain of custody is maintained. A standardized form should be utilized. And yes, you can FedEx computers/cell phones/media etc. and maintain chain of custody using your form and the FedEx tracking numbers.
- If the other side is claiming that production is too expensive or unduly burdensome, you always have the option of looking like the "good guy" by agreeing to forensic "sampling" of the evidence. As an example, if you claim the defendant has in its possession information belonging to your client, it is child's play for a forensic technologist to go in and find files, databases and potentially proprietary information as identified by your client. After that, the court is likely to be very impatient with the defendant's counsel bleating about expense or burdens when relevant evidence (and pilfered data) is clearly extant.

**The analysis of the evidence isn't just for your forensic technologist – you need to get involved too!**

- Make sure you are getting a true forensic image, especially if you are potentially going to be in court. A genuine bit-by-bit image is not a copy or a Ghost image (made with Symantec's Ghost product) but is made using specialized forensic software such as EnCase or the dd function of Linux.
- Be sure you understand the cost for the forensic services so neither you nor your client will suffer sticker shock down the road. Many forensic technologists will flat fee the imaging of anything that can be acquired in their labs. This is because they can begin the acquisition and walk away to work on another case. However, if the forensic imaging is done on-site, the technologist must "baby-sit" the acquisition. If the acquisition involves servers, this must frequently be done on a weekend to avoid business disruption. Expect to pay time and half for this service.
- Once everything has been acquired, analysis is usually performed at an hourly rate. Here, trust is required. Make sure you have good references for your forensic technologist. There are those who will tell you their hourly rate is \$200 but they will start their clock when they arrive at 8 a.m. and turn it off at 6 p.m. when they leave without any regard for the time spent at lunch, chatting with their spouse, checking e-mail etc. They will also charge for the time a search is running, even though the process is automated and they can work on another case. Reputable technologists will only bill you for time spent working on your case. They may charge \$350 an hour as opposed to \$200 – and yet you will end up with a smaller

total bill because the billing is honest. As with everything else in life, *caveat emptor*.

- Understand that your technologist isn't going to be able to give you a very precise projection of analysis time (except in rare cases, such as where only a single piece of e-mail is sought) at the beginning of the project. Give them a day or two of analysis to see the "size of the elephant" and then they will be able to give you some sort of reasonable estimate as to the time that the project may require in all but the largest cases. Once search terms have been run, they will know if they have 10 hits or 10,000 and likewise will know how much data they will need to review and potentially extract for you. To give you some idea of general costs, we generally tell folks that analysis in small cases (e.g. divorce, criminal, small civil matters) will typically run \$4000-\$8000. If, after wading into the evidence, we find that more work is involved, we alert the client before spending more monies. Often the client will wish to review the evidence procured thus far before determining whether more funds should be allocated to the effort. The #1 complaint about computer forensics and electronic evidence companies is that costs spiral out of control.
- Search terms should be developed with the assistance of your technologist and, if the firm has a lawyer on board (which is very handy for litigation support), with that lawyer. This too will keep costs down because they will look at your proposed list of keywords and tell you which ones may not make sense. As a for instance, searching for common names, such as Joe or Mary, is likely to result in a boatload of irrelevant information. Likewise, if you search on the word "system" on a computer hard drive, you will be swamped with hits that are meaningless to your case.
- It is prudent to give your technologist a statement of the facts in the case or a copy of (at least) the initial pleadings. When technologists understand what is relevant, they are going to do a far better job for you. Once again, if there is a lawyer at the firm, he or she will help devise strategies for effectively searching the evidence and therefore cutting costs.

### **How are you going to manage and review the data?**

- In small cases, lawyers can and do review the evidence themselves. It is simple enough if there is a limited amount of data. Your technologist will extract the relevant evidence from the proprietary (and very expensive!) computer forensics software (which you cannot read, not having the software) and put it in a form that you can read.
- Where the data is large or complex, you will need to determine whether you have the in-house resources to manage it, perhaps using software such as Summation or Concordance. If you have a fleet of paralegals to input everything, you may be just fine following this course.
- If you have a big case with terabytes of data and you lack internal resources, you will need to hire an electronic evidence company. Mind you, many companies, but not all, do both computer forensics and electronic evidence management. Here is the basic dividing line between the two fields. Computer forensics has to do

with the preservation, acquisition, extraction and the presentation of evidentiary findings for the court via a forensics report and/or expert witness testimony. Electronic evidence companies generally manage the evidence after it is extracted. Costs here vary widely, and once again, referrals are your best bet to avoid runaway costs.

- Are you collaborating with colleagues from different offices on the case? If you are, you may also need to have a data hosting company, which can securely place the evidence on the Internet for review by authorized parties from any location.
- If you are the party required to produce data, you will need to make sure you understand what format it is to be produced in. The new Federal Rules of Civil Procedure, expected to be in place by December 2006, will require that you produce the data in native format, absent an agreement to the contrary. Producing in native format keeps the metadata intact, but can be problematic if the recipient doesn't have the software with which to read the data, as often happens with proprietary programs. Production in TIFF format (essentially taking a picture of the evidence), which happens often, means the metadata (who authored the document, when it was created or last accessed, etc.) which accompanied the document, spreadsheet, etc. is lost to you.
- Make sure you are protecting privileged information when you produce documents. While the new Federal Rules will allow you to "call back" privileged information that was inadvertently produced, the horse has now left the barn. Far better to carefully review the evidence prior to production to screen for privileged documents and communications.
- If you are dealing with massive amounts of data, consider whether you want to do a "rolling production" so you can demonstrate that you are attempting to cooperate fully and quickly with any discovery requests. The process of data production in large cases can be incredibly time-consuming and judges are usually happy to work with a rolling production schedule, so long as timetables are met!
- If the discovery request is unduly burdensome or expensive, perhaps because the deleted data requested exists only on backup tapes or legacy systems, raise that issue early and be cognizant of the principles of cost-shifting as articulated by *Zubulake v. UBS Warburg*.

Is there a real gospel for best practices in electronic evidence? Not yet, but many groups are attempting to devise them. The Sedona Conference has done the best job so far and many legal entities, including the American Bar Association, are following in its wake. For more information about the work of The Sedona Conference and its publications, visit <http://www.thesedonaconference.org/>

In the meantime, following some of the bullet points above will give you at least a rudimentary map for proceeding through the e-evidence maze. If you should get lost now and again in the maze, don't worry – you have lots of company.

*Sharon D. Nelson, Esq. and John W. Simek are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax,*

*Va. (703) 359-0700 (phone); (703) 357-8434 (fax); sensei@senseient.com;  
www.senseient.com.*