

ELECTRONIC DISCOVERY IN EVERYDAY CASES: PRACTICAL GUIDANCE IS AN ANTIDOTE TO FEAR!

By Sharon D. Nelson, Esq. and John W. Simek
© 2007 Sensei Enterprises, Inc.

The smaller the law firm, the more paralyzing the notion of electronic evidence seems to be. Solo practitioners, in particular, seem to writhe in agony when confronted with cases involving e-evidence. How afraid are they? The authors have actually overheard two solo attorneys conferring in a courthouse corridor, exchanging mutual promises: “I won’t go near electronic evidence if you won’t.” “Absolutely, you have a deal.” Ethical implications of that conversation aside, the fear it reflects is all too common. Below is a wealth of practical advice regarding electronic discovery for the solo and small law firms handling electronic discovery.

We live in a world where all the studies agree that more than 93% of our information is generated electronically and will never be converted to paper. That statistic alone makes it clear that in many, many cases, electronic data will be pivotal.

It may well be that the mega-cases are part of the reason for the panic response felt by so many lawyers when confronted with electronic evidence. Without question, cases involving Fortune 500 clients and their pricy electronic discovery firms tend to rack up huge bills. The price range can be in the millions – six figure cases are garden variety. This is daunting, but rest assured, there is another world out there – one in which small electronic discovery firms work with solos and small firms on a much reduced and inexpensive scale.

We should note that computer forensics is typically the starting point for electronic evidence in small cases as it “captures” all of the electronics and not just that which is visible to the user. Some cases may not even need computer forensics and you can move right to the harvesting of electronic data.

So what is a small case? Here are some common examples:

1. A divorce with some assets, but the parties are not millionaires. If their assets are small enough, they can barely afford an attorney, much less a foray into electronic discovery.
2. A breach of contract suit between an individual and a small company.
3. Suits involving defamation or slander, where neither is a large entity.
4. Criminal matters involving the possession of child pornography or online stalking.
5. Theft of proprietary data – again, where neither party is a Goliath.

In small cases, the cost to do electronic discovery should fall, most of the time, under the \$10,000 mark. Mind you, that’s a ballpark – there are small cases that turn out to have unexpectedly large volumes of data – or perhaps the information to be unearthed is

complex and in many different places. Nonetheless, if you have a trustworthy vendor, you can expect most truly small cases to fall under \$10,000 provided that only a computer or two is involved. If there are a handful of computers and not a vast volume of data, you may find yourself in the \$10,000-\$20,000 range. Most vendors will flat fee the imaging if it can be done on their own premises, usually charging \$500-\$1000 per hard drive. Hourly rates for analysis are usually in the \$250-\$350 range.

The hardest part of ED, from the point of view of a honest vendor (and we use that term pointedly, since spiraling costs are the #1 complaint against ED vendors) is that you can never be sure exactly what you're dealing with when you first get into a case. If you know you only have a computer or two to analyze, most of the time you know the case will be a small one. However, it doesn't take many more machines and case complexities to ramp up the price.

Understandably, lawyers want their experts to give them a quote. Remember the line from "Star Trek?" Mr. Spock intones gravely to Captain to Kirk, "I will try to give you my very best guess." Well, that's what you're going to get. A principled company will give you their very best guess and then tell you that that's exactly what it is, a best guess.

Happily, once the forensics acquisitions are done and they are immersed in the case, they will generally know a great deal after 6-8 hours and can provide a far better estimate of ultimate costs. Now they have a sense of how much data they are dealing with and how difficult or easy it may be to find and export the data into a format that the attorney can use to review it.

Therein lies another challenge for the small firm attorney. What format do you want electronic evidence in? The vast majority of these attorneys have no access to big name e-discovery reviews tools – in fact, only a tiny fraction of them even have Concordance or Summation (two of the more well used ED tools). All this is less of a problem than you might imagine. Again, small cases are a beast unto themselves. With a limited amount of volume, it is simple enough for your computer forensics company to extract the relevant evidence and place it on a CD or DVD in a format that you can easily open using Word, Outlook, Acrobat, Internet Explorer, etc.

Better yet, your expert can give you a full report containing hyperlinks to the evidence so you can go through the story from beginning to end and take a look at the e-evidence at various waypoints along the journey. As an example, your expert may conclude at the outset that there is evidence of adultery and dissipation of marital assets. From there, the expert report may reference a volume of correspondence between the defendant and a particular paramour, then giving you a link to those e-mails so you can review the trail of cybersex and rendezvous arrangements in sequence. Perhaps there is evidence of assets hidden in off-shore accounts followed by a link to the Internet evidence showing the deposits in the account. Possibly there are documents in which various assets are listed with a link to those. These reports can be quite tidy and useful. Without a lot of technological know-how and skill, an attorney can review and hone in on the facts that are most relevant to the case.

Sometimes, you may look at the evidence in the hyperlinks and be confused by what you see. No worries, mate, that's why you have an expert. Just pick up the phone and your expert can talk you through what you're looking at piece by piece. Frequently, attorneys are confused by information found in "slack space" (we promise not to give you any ultra-technical definitions here). Slack space contains data that has been previously deleted and is partly but not wholly overwritten. Sometimes, you may find something that's quite the smoking gun ("Robert, we've been lovers for four years and I'm so tired of waiting") but you cannot attach it necessarily to a person or date because of the information around those words has been overwritten. Still, if the suspect paramour is named "Robert," this evidence is fairly persuasive.

Whether the case involves family law, business law, or criminal matters, never assume you know all the relevant e-mail addresses. Trust us, when someone crosses over to the dark side to do something they shouldn't, it is common practice to do so under something other than their normal e-mail address. The guy who steals a client database from his employer almost invariably has a web-based e-mail account such as gmail or hotmail and sends the data to himself at home. Likewise, a wandering spouse is very likely to use an e-mail that their other half doesn't know about.

Another thing that is often overlooked in small cases is the whereabouts of the evidence. The normal process is to fixate on an individual's computer. A great place to start, but does that individual use other computers, at home or at work? Do they use thumb drives or iPods (iPods have become a fast growing phenomenon in computer forensics – remember, they carry data of any kind, not just music!)? Do they have a cell phone? Oh my, the text messages we have seen that scorch our eyebrows! And don't forget the disks and CDs that they have cluttering their desk. So think technology, but think globally – no tunnel vision.

Another oft-asked question: can my client install spyware and monitor their spouse to gain the evidence they need? Though there is not yet a federal spyware act, and state laws vary widely, the answer is no, no, no! The use of spyware means that you are intercepting electronic communications, forbidden under the Federal Wiretap Act. Even if it is inter-spousal, and both parties live in a state where spyware is not expressly forbidden, the federal law will still apply because the Internet is a vehicle of interstate commerce. Once you click "Send," even if the recipient is just a block away, your message might traverse communication lines in several states. We have seen any number of divorce cases where the adulterous spouse got a "free ride" because evidence gathered using spyware was held to be inadmissible – in our own state of Virginia, which has a state wiretap act, evidence gathered through the interception of electronic communications is expressly excluded, as it is in most states with similar laws. We have also seen parties to a divorce forced to take the Fifth Amendment in a deposition because they only found out subsequent to their use of spyware that they had committed a crime. In that case, not only does the adulterous spouse get off scot-free, but the wronged spouse may be charged with a crime. This is not a happy or fair outcome, but we see it all too often.

Do you really need to know the science of forensics to handle an ED case? Absolutely not – that’s why you have an expert. Having said that, the process (not the science) of the average case is not all that hard to understand. Generally, your expert will assist you first in locating all of the evidence. Let us say that a single computer is at issue and that a court has granted you the right to have your expert image the computer and analyze the evidence. The forensic technologist will carefully log the computer in on a chain of custody sheet and take photographs to document the computer and its condition (at times, we’ve even been able to document evidence of tampering via digital photos). The technologist will then do a forensic image of the computer, which is not a copy or a “Ghost,” but a bit by bit image of the computer. The data in the imaged computer is not touched at all – the imaging is done in a read-only mode. At the end there will be a mathematical algorithm (normally an MD5 hash – sort of a digital fingerprint) which precisely matches the MD5 of the acquired computer hard drive. Ordinarily, the expert will scan the evidence for any viruses or Trojans, which may have to be dealt with. Sadly, the next step is to scan for child pornography using hash values for known images. Following this point, the image will be held under lock and key until analysis is authorized.

Analysis presents its own set of problems, but generally the expert can ferret out the correct search protocol by asking the attorney questions. Again, the attorney is not expected to be savvy in computer forensics – if the attorney can explain clearly what he or she is looking for, the expert will tell you how best (and most economically) to search the electronic evidence. It is helpful if the expert is given the original pleadings in the case, as well as any other documents that may be pertinent to forming a search protocol. If money is a huge concern, make sure you are narrowly tailoring the search. The greater the volume of responsive data, the greater the cost to bookmark and extract search results.

If you actually get to trial, make sure you adequately prepare your expert. There is nothing worse than listening to an attorney fumble for words about a subject he doesn’t understand, often thereby confusing the very expert on whose testimony he depends. Forensic technologists who are frequently expert witnesses can help outline the questions for you, so that you appear to be “telling a story” which can be readily understood. There is always a danger that this sort of technical testimony is obtuse to a judge or jury, so keep it straightforward and simple – and in plain English. If you are comfortable with PowerPoint, most forensic technologists can help you translate any case complexities into an easy-to-understand presentation format.

If you’re just taking baby steps into ED, educating yourself is important – and not nearly as hard as you might imagine. These days, there are many CLEs on the subject of ED – and often they can be found online. Books and periodicals abound, as do online resources. A very good starting point is <http://www.discoveryresources.org>. If you want to get a flavor for ED in case law quickly, we recommend reading the whole line of *Zubulake* opinions (there are 7) in *Zubulake v. U.B.S. Warburg*, a standard discrimination case which resulted in writings which are still referred to as the “gold standard” in ED. The Southern District of New York really put itself on the ED map with this series of cases. If metadata really confuses you (or if, horrors of horrors, you don’t know what

metadata is) a great guide to metadata can be found in the *Williams v. Sprint* case, 230 F.R.D. 640 (D. Kan. 2005). Finally, you can download all of the ED work of The Sedona Conference at <http://www.thesedonaconference.org/>. Courts very frequently cite to the works of the Sedona Conference and woe betide the lawyer who is unfamiliar with its guidelines.

The most important thing you can do if you are a new voyager in this esoteric land is to find an expert you trust. Believe us, experts are used to hand-holding and patient teaching. Good experts will also have forms that you can use as a template for your cases, and will guide you at each juncture of your case. Once you've done a few ED cases, you'll be surprised at the extent of your knowledge. Remember the immortal words of Confucius: "What I hear, I forget, what I see I remember, what I do, I understand." Immerse yourself in ED, get a few cases under your belt, and you too will join the legions of lawyers who have learned to travel comfortably in the world of electronic evidence! Happy voyaging.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com