

SHARING THE PAIN: BAR ASSOCIATIONS AND ELECTRONIC DISCOVERY



NABE

AUGUST 8, 2007

Presenters:

**Jim Calloway
Lincoln Mead
Sharon Nelson**

SHARING THE PAIN: BAR ASSOCIATIONS AND ELECTRONIC DISCOVERY

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

“Not only do I not know what's going on, I wouldn't know what to do about it if I did.”

- George Carlin

Carlin's quote is a great description of how most lawyers feel about electronic evidence. This subject is so terrifying to many lawyers that they simply avoid it. Preparing for e-discovery to them is akin to preparing for Armageddon. We've even seen lawyers so afraid of it that they acknowledged that they got drunk when they realized they'd have to deal with it in a case. Which brings to mind another Carlin quote: *“One tequila, two tequila, three tequila – floor.”*

Electronic discovery causes great pain. Most readers can probably relate to the pain of getting up in the morning and stepping on the scale, only to groan thinking of how unkind the years have been. At some point, that miserable scale and its dismal number cannot be avoided and no matter how loathsome the idea of counting calories and exercising regularly, you just don't have a choice unless you want to play roulette with the Grim Reaper.

Having successfully avoided electronic discovery for a very long time, bar associations and their members have finally woken up to the reality that no lawyer can practice in this day and age without confronting the equivalent of the diet and the exercise: in this case, a serious study of the subject of electronic discovery (ED) and at least a fundamental understanding of technology. Muttering imprecations under their breath, lawyers have been showing up in CLE classes throughout the country, many expressing serious fear about a world they do not understand – some worried that they may never understand it.

Not only do bar associations have a mission to help educate their members about ED, they need to swallow the bitter pill themselves. Bar Associations get sued. Sharon's did, while she was President. Having drawn the short straw, she was nonetheless relieved that the discovery involved was minor and did not involve ED to any significant extent. The Bar got lucky. A mere \$10,000 later, the frivolous suit against us (for obeying an IRS order to garnish an employee) was dismissed.

In today's litigious world, when someone sues because the bar association's judicial screening committee gave them an unfavorable rating, or an employee sues for discrimination or alleging a hostile workplace, the consequent discovery is very likely to

involve electronic evidence. Are bar associations, in general, even close to being ready for this possibility?

Perish the thought. We have yet to see a single bar association that has taken ED seriously on its own account. Bar associations are happy to provide CLEs for their members, but do they have a document retention policy in place? Are they prepared for the imposition of a litigation hold? Have they the slightest notion of how to forensically image or cull their data for relevance? Such questions tend to invoke full scale panic in bar association executive directors.

Even when the questions are more basic, there is apprehension. Does your bar association mandate the deletion of unneeded records? Does it even limit the size of employees' mailboxes. Or does it, like so many law firms, simply keep all detritus and, when the hard drive is full, simply move it to a larger hard drive? In truth, it is very simply to do exactly that because storage is so cheap. Only when electronic discovery becomes an issue do bar associations realize how expensive it is to embark on the electronic equivalent of dumpster diving.

Review of all those gigabytes of data is incredibly costly. The painful lesson is that garbage needs to be thrown out. Like any other organization, bar associations need to determine what data needs to be kept for statutory or regulatory reasons, what data needs to be kept for historical and business purposes, etc., etc.; then toss the rest. E-mail storage should be limited to enforce clean up. A document retention policy, even a simple one, will help as long as compliance is monitored and enforced.

Think of all data as potential future evidence and the wisdom of pruning it becomes apparent. Once you have limited the scope of available data, it is wise for bar associations to have a litigation hold policy in place as well. A bad time to develop this policy is directly after receiving notice of the lawsuit. If the policy is in place beforehand, you have only to consult it to know what actions need to be taken.

A litigation hold goes into effect when you know or should have known that a regulatory action or lawsuit was likely. Not every disaffected employee will trigger such a suit, but if internal administration actions have already been instituted, it is probably time to think about whether the litigation hold needs to be put in place.

Your litigation hold policy should identify which folks will be on the litigation hold team – perhaps the association president and vice president, the executive director, outside counsel and one staff member responsible for communications. These folks will determine at the outset of a litigation hold what documents must be preserved, who the key players are (their local hard drives may need to be preserved or forensically imaged), and what attorneys or electronic evidence experts may need to be involved. The team will see that preservation notices are sent to all the appropriate parties, including third parties who may hold the association's data, such as outsourced web application providers.

The most important thing for that team to remember is that it must document, document, document each of its steps. A court reviewing the preservation methods will inevitably look at the good faith and reasonableness of the steps taken. If there is a clear attempt to do all the right things, an inadvertent stumble is unlikely to be punished by sanctions. However, a lot of fumbling in the dark and spoliation is a different matter. Courts have lost patience with those who refuse to prepare for e-discovery and do not self-educate once the need arises. Million dollar sanctions are now run of the mill, though a court sanctioning a bar association would undoubtedly tread lightly as bar associations are generally as poor as the proverbial church mice.

Attached to this article are materials which will aid a bar association in preparing for e-discovery as well as considerations for selecting an appropriate computer forensic expert, if needed. These same materials, as well as many others, are useful for bar members as well.

Virtually every bar association has as its mission, service to its members, including the provision of continuing legal education. In this complicated new world of electronic discovery, members are particularly in need of their bar's help. Although nearly all lawyers now use e-mail, that was not true a decade ago. Likewise, a decade from now, lawyers may have e-discovery well in hand – but that is certainly far from the case now.

Older lawyers tend to be clueless about e-discovery, including prominent attorneys who have never been particular tech savvy. There is still a large contingent of lawyers who are basically technophobic. They are having a very hard time with court cases that say, essentially, a company's lawyer is now responsible for understanding the network topology of her client when e-discovery is in issue, along with its backup system and any other arcane matters. This is quite terrifying to a generation of lawyers that can only barely manage to send an e-mail with an attachment and cannot convert a document to PDF without the assistance of staff.

Education is clearly the answer, and bar associations across the country have been scrambling to assist their members in coming up to speed. The new federal rules pertaining to electronic evidence, which came into effect December 1, 2006, have been the impetus for much of this education. The first course we all saw from bar associations was "The New Federal Rules and Electronic Discovery" in one form or another. Now that most lawyers have had this 101 training, it is time to take it to the next level.

Advanced courses are sorely needed, to discuss in detail the preferred format of production (native, TIFF, PDF, etc.), metadata in ED, how to prepare for the Meet and Confer, a review of court guidance since the rules came into effect, a report on what the states are doing, guidance from both federal and state court judges, how to answer an electronic discovery RFP (yes, law firms are now receiving them!) how to authenticate electronic evidence, the use of subpoenas to ISPs, selection of electronic discovery experts, the presentation of electronic evidence in court and the science of computer forensics. More and more, attorneys are concerned that they are essentially receiving the

same information in the ED courses they attend, without receiving the higher level information that they now need.

Who should teach these courses? Litigators who have experience, judges, professors and vendors who are known to teach rather than sell. Who can genuinely teach computer forensics without actually doing it every day? But be mindful of instructing any vendor/presenter that selling will not be tolerated in an educational setting. NABE itself is a great resource for good presenters – simply post a question to the list about those who have expertise who are somewhere in your region or can travel to your locale.

Quite useful to members would be a list of links to electronic discovery resources on the Internet. A good start to compiling such a list would be perusing www.discoveryresources.org and www.denniskennedy.com and www.abanet.org/tech/ltrc/fyidocs/ediscovery.html. While a live CLE, which not coincidentally makes money for the bar, is always desirable, it is also helpful to compile links to reputable online CLE providers, which have the ability to frequently offer higher level courses.

At the outset of this article, we talked a good bit about the need for bar associations to prepare themselves for e-discovery. Make no mistake – law firms need the same help. Their houses are in disarray as well, with little internal attention paid to ED readiness. The focus has, understandably, been on making sure that the lawyers are prepared to help their clients. There has been a steep learning curve for many lawyers. To date, the authors are aware of only two cases where sanctions have been imposed on law firms, but undoubtedly that number will grow. There have been many, many cases where the lawyers were chastised for their clumsy handling of electronic evidence, but the courts have been loathe to sanction them unless bad faith seems to exist.

The focus on serving clients has resulted in a marked improvement on lawyers' ability to serve their clientele but it has also meant that very few firms (especially solos and small firms) have done anything in the way of developing document retention and litigation hold policies. Bar associations will help their members by ensuring that they are well educated about the perils of “doing nothing” with respect to their own law firms. Law firms have begun to hoard their electronic data with the same zeal as they hoard their paper. Most seem blithely unaware of the costs associated with reviewing and producing all that data in the event of a lawsuit.

The world has changed forever. Studies vary a bit, but it is generally agreed that 95-97% of all data is now created electronically. Of that, only a scant portion (some studies say as little as 3%) will ever be converted to paper. In law firms, as we all know, that number will be higher, but most of the rest of the world is keeping electronic data electronic. In this new world, we still from time to time hear lawyers agree in courthouse corridors, “I won't go near electronic evidence if you won't.” There are clear ethical implications of such an agreement, but pragmatically, such agreements no longer make sense. If the question at issue is whose dog bit whom, electronic data may be irrelevant. However, in ALL cases, it is imperative to ask if electronic evidence may exist and to search it out if it

does. Undoubtedly, we will see malpractice suits alleging that the attorney failed to investigate electronic evidence.

For bar associations to genuinely provide service to their members, it is imperative that they get them to concentrate on the importance of e-discovery and to make them familiar with the process. Most attorneys have no clue whatever about how to fashion interrogatories with respect to a party's network infrastructure, and yet this is precisely what they must do early on in a case where electronic evidence is in issue. It will take some time, and there will be members who are resistant, but the best way for a bar association to serve itself and its members is to be at the forefront of emerging developments in electronic discovery.

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

ELECTRONIC DISCOVERY COMES OF AGE: THE FULBRIGHT JAWORSKI STUDY

By Sharon D. Nelson, Esq. and John W. Simek

© 2007 Sensei Enterprises, Inc.

Ah, the rites of passage. A young man turns 21, goes on the town with his friends, tosses back 21 shots, throws up and passes out. Happy Birthday son, if you can remember it. Variations on this scenario happen nationwide every day. Has Electronic Evidence come of age? If so, how has it marked its rite of passage?

It was only eight years ago that we began lecturing on the subject of electronic evidence. At the time, we ran one of a handful of computer forensics/electronic discovery companies across the nation. When we warned audiences that **all** lawyers would have to become familiar with e-discovery over the next few years, we were greeted with cavalier disregard. "I don't think so – folks will pretty much go on practicing law the way they always have," was a common remark.

It was only three years ago that we lectured to a group of Circuit Court judges in Southwestern Virginia. While our hosts were uniformly gracious, they were also uniformly adamant about electronic evidence and courtroom technology. "Not in my courtroom!" several of them said firmly.

My, how times change.

Most federal court litigators have come to accept electronic discovery as a daily fact of life. While the use of e-evidence has seeped more slowly into state courts, virtually all litigators have now, however reluctantly, begun the process of educating themselves about electronic evidence.

The Fulbright Jaworski Study: ED Grows Up

The recent release of the second annual *2006 Litigation Trends Survey* by the international law firm Fulbright & Jaworski L.L.P. has made it eminently clear that electronic discovery has indeed come of age. Some things haven't changed - to no one's surprise, we are an intensely litigious society.

The survey included over 300 corporate counsel. These were not small businesses, to be sure. The median company reported annual gross revenues of \$484 million. Still, it is startling to read that the average company in the survey juggles 37 lawsuits at a time. For \$1 billion plus companies, that number grows to a staggering 147. Keep sending Jack and Jill to law school!

Here's the ED kicker: For corporations with over \$100 million in revenues, the greatest concern of the responding general counsels and CEOs was electronic discovery. For those under that mark, the greatest worry was compliance issues. If you think about it a moment, failure to comply will almost invariably involve electronic evidence in the ensuing compliance actions or litigation. Taken as a whole, electronic discovery has indeed, in its own fashion, painted the town red – in this case, the color of panic.

What a departure from the good old days the study reveals. 80% of the respondents now have document retention policies and 75% have litigation hold policies. Still, the respondents worry about the quality of their policies, the enormous costs of electronic discovery and the sanctions that may accompany a failure to live up to statutory, regulatory and case law requirements.

What Does All This Mean to Smaller Companies and Their Law Firms?

The big boys felt the impact of ED while most lawyers slumbered on, practicing law without a thought to electronic evidence. Only a fool would suppose that ED will stay in the stratosphere with the large firms and their clients. Inevitably, ED will drift downwards and seep into more and more small cases.

Our current caseload of forensics/ED cases may be instructive. Currently, about ¼ of our cases are divorce cases. If you're surprised, think about how often people e-mail, IM or text message their lovers. It's where the evidence is. Next time you see someone using two thumbs on a BlackBerry, you might justifiably wonder if they are telling some special someone what kind of new erotic treats they have planned for their next rendezvous. Trust us when we tell you that people will write **anything and everything** to their paramours. Our eyebrows are permanently singed from reading their missives.

Criminal cases comprise the next 25%. A depressingly large chunk of that is child porn cases, followed by everything from stalking to embezzlement to murder. Business litigation constitutes about 25% - software that doesn't work as advertised, employees who are funneling company data elsewhere, competitors that have pilfered proprietary data, etc. The final 25% is a hodgepodge of everything from terrorist cases to defamation to people who have forged wills. Perhaps 3 or 4 of all these cases involve really significant dollars. The rest are really the everyday cases that comprise the law practice of the solo/small firm practitioner – with one notable difference. ED is now a critical component. No doubt this is the tip of an immensely large iceberg. We are in fact seeing the beginning of seepage of ED into everyone's law practice.

But make no mistake about it. Most cases in our area still go from A to Z without anyone thinking about e-evidence. But the times, they are a-changing.

Fear is a Great Motivator

Lawyers have not precisely embraced electronic evidence. Their trepidations about dealing with e-evidence have only slowly abated. Their new-found willingness to deal

with e-evidence seems to stem larger from fear – that they will be guilty of ineffective assistance of counsel if they ignore it, or that the other side will find a “smoking gun” unbeknownst to them. If you want to be a good lawyer, and serve your client well and competently, there is no longer any way to evade the fact that e-evidence is a factor in a growing number of cases.

Still More Statistics

Statistics, as they say, lie. They can be manipulated to prove anything, and often are. However, no matter whose statistics you believe, all of the recent studies show that somewhere between 93-97% of all information is now created electronically. It is commonly accepted that less (some would say MUCH less) than 3% of that information will ever be converted to paper. That being the case, what lawyer worth his/her salt can afford to ignore at least the possibility of electronic evidence being relevant every time a new case is opened?

We are now sending more than 4 trillion e-mail messages a day in North America. Worldwide, we are producing 1-2 exabytes of information per year. If you're scratching your head wondering what an exabyte is, it is equal to roughly 1 trillion books.

You Can Run, But You Can't Hide

Electronic discovery's rite of passage is ongoing. However, as the Fulbright Jaworski study makes clear, ED has arrived in force. Undoubtedly in the last several years, the general counsels and CEOs of major corporations have felt very much as though they had just chugged 21 shots, though not exactly in celebration of ED's coming of age. More likely, they feel the headache/hangover effects of ED, which came on suddenly with all the force of a tornado and with nearly as little warning.

Perhaps the best thing for solo/small firm practitioners to do is heed carefully the various disasters that have befallen their larger counterparts as they became the first to encounter the full breadth and depth of ED's impact. On a smaller scale, the very same thing is likely to happen to anyone not prepared for electronic discovery. You can wish it away, will it away, even pray it away, but electronic discovery is here to stay. Just look at all the ED companies that have sprung up faster than chickweed. Mind you, many of them fail rapidly in this volatile new market, but for each one that fails, two seem to take its place.

We all wish that electronic discovery were more settled, that laws and regulations were more uniform, that case law wasn't all over the map etc. But ED is only just of age, brash, heady and volatile as any young man on his 18th birthday ever was. If you thought you could avoid ED and keep practicing law as you always did before, you'd better do a shooter or two yourself to ease the pain. ED is coming to everyone's town!

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

Finding Wyatt Earp: Your Computer Forensics Expert

By Sharon D. Nelson, Esq. and John W. Simek

© 2007 Sensei Enterprises, Inc.



Wyatt Earp, c. 1886

You are about to enter the OK Corral of litigation. The stakes may not be life and death, but they're high. You have a litigation team – your own version of Doc Holliday, Virgil Earp and Morgan Earp. The other side is also formidable, the modern day equivalent of the Clantons and the McLaurys. Both sides are well armed and ready for bloodshed.

In the ensuing battle, more often than you might imagine, the winning difference in cases involving electronic evidence is the skill level of the computer forensic expert. Whose expert will the jury or judge find more credible?

It is at this juncture that you hope fervently that you haven't bet your client's monies and case on Ike Clanton. You hope your guy is Wyatt Earp himself, imperturbable, flinty-eyed, and deadly accurate. But where oh where do you find the Wyatt Earps of computer forensics?

Scarcer than rubies are talented computer forensics experts who are also skilled at writing expert reports and giving court testimony. So how do you find a good expert when you have electronic evidence in issue? This can be a daunting task and the right selection may depend upon a number of factors including what's at issue in the case, the budget, the geographic location of the expert, and balancing the relative credentials of the experts under consideration. In short, reach for your bottle of Advil. Mistakes are frequent.

Here are the extremes. At one end, you have the major players – with big price tags and a horrendous disparity of quality between their employees. At the other end, you have Joe, formerly a plumber, who fiddles with computers at night and thinks that computer forensics is cool. He takes a course in it, perhaps even gets a meaningless certification from the vendor, and then promptly hangs out his shingle, advertising his service at “blue light special” rates.

Do you pay a fortune for the big name players? Do you take a chance on Joe and his brethren?

Regardless of the size of the firm you choose, here are some of the factors you should consider in selecting the specific forensic technologist expert for your case:

1. **Forensics certifications.** Currently, the most prestigious certification available to private firms is the EnCE (EnCase Certified Examiner) issued by Guidance Software. Another certification rapidly gaining respect is the Certified Computer Examiner issued by the International Society of Computer Forensic Examiners (ISFCE). More certifications are emerging and will gain credibility over time, but in the private sector, the EnCE and the CCE are the certifications to look for. A caveat: many less than honest folks will claim certifications on their CV when the truth is that they took classes or had training courses – no real meaningful certification was granted, just a “certification of attendance.” If you see a certification you don’t recognize, find out whether a written exam was required. Did the applicant have to prove some minimum time that he/she had been involved in computer forensics? Was the expert certified in computer forensics or merely in the use of a particular forensics tool? What organization issued the certification? Who was on the faculty? Was a practical hands-on component part of the testing? Is there a recertification component?
2. **Technical certifications.** A good forensic technologist will have a lot of letters after his/her name, indicating a broad range of certifications with a number of different technologies. If you see no certifications, or a “base-level” certification (such as A+), you do not have an individual with a wealth of experience. If the expert is (just by way of example – there are many, many valuable certifications) a Certified Novell Engineer, Certified Cisco Network Administrator, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineer, NT Certified Independent Professional and a Certified Internetwork Professional, you’ve got someone with an expansive technical background.
3. **The CV.** Get the expert’s CV early on and study it. Don’t be afraid to ask questions. Does it show that the expert has spoken at a lot of seminars and/or written a lot of articles? Those who present or teach frequently and have to answer questions on the fly tend to be excellent testifying experts. Also, teaching and authorship frequently add credibility with a judge or jury. What is the expert’s educational and professional background? Is this a broad-based technologist or someone who is a new college grad and wet behind the ears or with only a narrow sliver of technical knowledge?
4. **The Jack of All Trades.** Beware the individual who claims multiple disciplines. Whether a private detective, computer repairman, or software engineer, or some combination of many things, a forensic technologist worth having is generally billed as a forensic technologist and does not offer a Chinese buffet of services.
5. **Court Qualifications.** The last thing you need as an attorney is an expert who hasn’t qualified as an expert. Good experts have qualified in multiple courts and they are all listed on the CV. Mind you, most cases of any kind tend to settle, so

even the best of experts may only appear in court several times a year. However, it is wise to be wary of someone who has only qualified in one court – or none at all. You don't need a greenhorn cutting his teeth on your case.

6. **Confidentiality.** Remember the line from the gossip columnist in the movie *L.A. Confidential*? “Off the record, on the QT, and very hush-hush.” Not all cases are shrouded in secrecy, but a fair proportion of them are. There are well known figures getting divorced, major companies with proprietary information at issue, public figures in the headlines and people charged with felonies. Make sure the expert you pick has a confidentiality clause in the retainer agreement and don't hesitate to ask the expert to sign your own confidentiality agreement. Remember as well that the expert may be working your case with others and that the entire firm should have an impeccable reputation for keeping client secrets. During the course of a major case where the expert has been identified, the press will undoubtedly come sniffing around the expert probing for information. A good expert knows the standard answer, “I'm sorry, I have no comment” and is as immovable as the Great Wall of China.
7. **Geography may not matter.** How often attorneys forget that this is the electronic era! You can maintain chain of custody perfectly well by shipping a computer from California to New York if that's where the best expert is located. While it is true enough that local experts are often preferred where monies are tight and travel expenses may be in issue, many lawyers lose sight of the value of having the best possible expert, irrespective of location. If the case has a significant amount at state and/or may well end up in trial, it is a disservice to clients to restrict them to local experts. Those experts who are well known in the field have clients across the nation and beyond because their expertise is so often sought.
8. **English 101 and 201.** An expert MUST speak the English language. We have many wonderful friends who are of foreign descent and brilliant, but their English will not pass muster with a mixed ethnicity jury. Their accent is just too pronounced for many folks to comprehend, especially for those who may have learned English as second language. That's English 101, being able to speak the language clearly. English 201 is being able to speak about highly technical matters in lay terms, with analogies that a judge or jury can understand. Geek-speak is worse than useless in a courtroom situation. You will come to revere an expert who easily makes analogies in terms of TV, cars, sports and other things that represent part of Joe Q. Public's everyday life.
9. **The price tag.** Computer forensics is not cheap. Small cases may run in the \$5,000-\$10,000 range, but larger cases can hit six figures with astonishing rapidity. It is almost never possible to quote a probable final figure, because the technologist has not yet seen the “size of the elephant.” It will generally require some time into the case before it is possible to let a client know how much work will ultimately be involved. It is, as we all know, often the same predicament lawyers face when trying to give clients a rational estimate. As a general rule, the

larger the forensics firm, the larger the bill. It is not uncommon to pay as much as \$500/hour in the largest firms. In high quality but smaller firms \$250-\$300/hour may be a more common charge. If the firm you're looking at charges less than \$200/hour, you probably want to raise your eyebrows and seriously investigate the firm credentials, references, number of courts qualified in, standing in the industry, etc. Heed this advice well: some technologists bill fairly. They turn their clocks off while a process is running and go work on someone else's case. They account for their time accurately and precisely. On the other hand, there are those (often with lower rates), who charge you for every moment they are at work – and sometimes beyond. We have seen countless invoices for 9-10 hours a day at work, with no time removed for going to lunch, bathroom breaks, chatting with colleagues, meetings, etc. Frequently, we have found that those with lower rates compensate by billing for more hours. A conundrum for a client. Is the lower rate really going to mean a lower bill? Or will the higher rate, accurately applied, result in a smaller total? In the end, getting references is your best bet here. *Caveat emptor!*

- 10. References, references, references.** There is no better way to secure a good expert. Ask your potential expert for references and then make sure you follow up with those references. Did the expert do a thorough, professional job? Was the expert responsive when contacted? Was the work completed on time? What was the quality of the expert's report? Did the expert make a credible witness? Was this an expert amenable to being "spun?" Experts who are "experts for hire" are a nightmare in court. If your candidate has the attitude that "the truth is the truth," you may not want that truth in court, but at least you will know the realities of your case, its strengths and weaknesses. Did the expert stay within budget (not always possible) or at least alert the client of additional costs before incurring them? Perhaps the number one complaint heard about experts involved in electronic evidence is that costs spiraled out of control without notification to the law firm, resulting in a client highly perturbed with its bill --- and its law firm.

At the end of the day, you want a good result at a fair price. Don't be penny wise and pound foolish. Pay good people good monies and you'll have a credible result – you may not get the answers you want, but what you get will hold up in court. Make no mistake about it – in e-evidence cases, it frequently comes down to a duel between the experts. Your guy gets blown away or their guy gets blown away. What you want is for your guy to be Wyatt Earp and the other side's guy to feel like one of the Clancy brothers staring down the barrel of Earp's "Peacemaker." You will be a lot happier in the courtroom's O.K. Corral if you have the biggest gun!

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

The Countdown to Zero is Over: The New Federal Rules of Civil Procedure

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

Some lawyers are simply terrified. Most are worried. A few blissfully assume that they can go along in splendid ignorance, as they always have.

You may not need to quake in your boots, but if you practice in federal courts, it is well nigh time to bring yourself up to speed on the new Federal Rules of Civil Procedure, which went into effect on December 1, 2006.

So why are otherwise stalwart litigators quaking in their boots? For the most part, it is the recent court-imposed sanctions that terrify them. The Morgan Stanley case, all by itself, caused a ripple of dread throughout the litigation realm.

By no means is Morgan Stanley alone. There is now a raft of cases out there, all bearing the same message to attorneys: Comply with e-discovery required practices or pay the piper. Sanctions have varied – most fines have been assessed against clients rather than attorneys, but judges have indicated that may change if the attorneys don't start toeing the line. More and more, judges have liberally handled out "adverse inference" instructions in cases of spoliation or "evidence gone missing," instructing juries that they may assume that the absent evidence was negative. Can you hear the other side happily exclaiming "SCORE!?" All of these penalties have been imposed without the benefit of having the new F.R.C.P. to back them up. Hence, the fear. Now that the duties are laid out clearly, what will it cost my client – or my firm – if I don't abide by them? Are malpractice claims a possibility for those who ignore the new rules? You betcha.

Mind you, nothing in the new rules is rocket science. But it behooves all lawyers in federal practice to understand the new rules before they become newspaper fodder as a result of their missteps.

So what do you need to know?

First and foremost, electronic evidence is now center stage. You must address it, and early on. No more agreements with opposing counsel that "I won't go there if you won't." No way, no how – you may not like it, but you're going to have to deal with it.

Though you need to read both the new amendments and the extensive commentary to them, here's a fast and dirty crib sheet.

ESI: WHAT'S IN A NAME? EVERYTHING.

Precise wording now counts. What we've all called electronic data for years now has the official moniker of "electronically stored information," or ESI. Get that right, and you're

already ahead of the crowd. Do you also remember how we all scrambled to insert in our pleadings a new, absurdly long definition of “document” that would include every imaginable kind of electronic information? No worries mate. From now on, “ESI” refers to all things electronic, whether you specify the nature of the information or media, or do not. The new rules are broadly written and the definition of ESI is, hopefully, so broad that it will encompass all sorts of technological change without the need for an amendment to the definition.

PRETTY PLEASE, CAN I TAKE A PEEK?

For years, opposing counsel has screamed about the undue burden of massive production. Under Amended Rule 34(a), where massive amounts of data may be in issue, you can now “sneak a peek” by sampling the ESI. If relevant information is found, game over – they have to produce. If it is not, you may have a very hard time convincing the court that you need still more data.

PICK ANY FLAVOR ICE CREAM YOU LIKE

Well, at least you can start out that way. Amended Rule 34(b) permits a requesting party to specify the format in which they would like to have ESI produced. Now, be wary - that isn’t precisely “endgame.” The other side may object to the format and some negotiation or a court hearing may be necessary. But the expectation on the part of electronic evidence experts is that the vast number of requests will be to have the data in native format, most often to preserve metadata or the ability to play with “what if” scenarios using the native format. If no format is specified, than the responding party is required to produce the ESI in the format in which is ordinarily maintained or in “reasonably usable” format. This amendment is expected to produce a few face-offs before case law settles the dust.

WE DON’T HAVE TO ANSWER YOUR STINKING QUESTIONS

This is true. Amended Rule 33(d) permits a responding party to produce ESI in answer to an interrogatory if the burden of deriving the answer will be substantially the same for both parties. A caveat here though - many attorneys suspect this is a minefield and would rather craft an actual answer rather than hand out data. If you choose to hand out data, the producing party must provide “sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained” and must allow the requesting party “reasonable opportunity to examine, audit or inspect” the records that are identified. Where privileged documents or proprietary information may be involved, allowing access to ESI could be the equivalent of opening Pandora’s box.

GIVE IT TO ME NOW!

Amended Rule 26(a)(1)(B) adds ESI to the list of what each party must disclose to the other during the opening stages of a case.

YOU CAN'T HAVE IT – IT'S INACCESSIBLE –SO THERE!

One amendment expected to cause some trouble is Amended Rule 26(b)(2)(B), which states that ESI need not be produced if the source is not reasonably accessible because of undue burden or undue cost. For instance, many companies no longer have the capacity to read some of their legacy back-up tapes. For years, it has been true that restoring ESI from tape was problematic, though the problems have lessened with technological advances. Still, it will take a number of court cases to sort out the definition of “inaccessible.” Saying data is inaccessible doesn't necessarily make it so, and the other side is likely to file motions to compel production. Saying it is too expensive may not work either – judges have become increasingly skeptical of statements that “it will cost millions of dollars” to restore ESI – they are beginning to demand alternative estimates from other vendors where they think the cost claims are excessive. Moreover, if the requested party can show that information is important, relevant, unavailable elsewhere, not such an undue burden considering respective resources, and that important issues are involved, the opposing party may be required to produce with all objections cast to the winds by the court.

PLEASE, PLEASE MAY I HAVE IT BACK?

Attorneys have lived in dread of having privileged documents inadvertently produced. Amended Rule 26(b)(5)(B) creates a “claw back” process whereby the producing party may inform the other side that privileged material has been produced, and the requester must “promptly return, sequester, or destroy the specified information and any copies it has” and “take reasonable steps to retrieve” any information already distributed. Of course, the receiving party may also bring the matter to the court if there is a dispute on the matter of privilege.

MY HOUSE OR YOURS?

The infamous “meet and confer” conference is going to be an earth shaker for many attorneys under the new rules, especially in jurisdictions where they could get away with an exchange of correspondence or picking up the phone and chatting with opposing counsel. Amended Rule 26(f) clearly states that that electronic evidence must be discussed at the pretrial conference and that agenda items must include: 1) the preservation of discoverable information; 2) issues relating to disclosure or discovery of electronically stored information, including the form in which it should be produced; and 3) issues regarding claims of privilege or protection as trial-preparation material, including whether to ask the court to include an agreement on non-waiver of privilege in an order.

Many parts of this new rule will compel interest, but here is our take: attorneys better make a quick call to their computer forensics/e-discovery expert and make sure that he/she attends this conference. Moreover, a senior representative from the IT department of both parties is going to be needed. If e-evidence is under discussion, the expert will

not, at that early juncture, have a full understanding of the IT infrastructure. Nor will the IT representative be qualified to discuss what is possible, desirable or best practice with respect to ESI preservation and production.

The heart of the new rule is an expectation that lawyers will work collaboratively and amiably early on to address e-discovery issues. We are not betting the mortgage money that this will go smoothly.

DEADLINE? DID I AGREE TO A DEADLINE?

Deadlines in e-discovery are ephemeral and subject to frequent morphing. However, Amended Rule 16(b) now insists that e-discovery and any claims or privilege or protection as trial preparation materials after production be made part of the scheduling order. Since even your experts may not know how much ESI there is to cope with in the early stages, this may be dicey. It is akin to Mr. Spock making “my best guess, Captain” and hoping for the best.

SOMEBODY THROW ME A LIFELINE!!!!

Somebody did, in the form of Amended Rule 37(f), at least – sort of. The so-called safe harbor rule says that “a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” Be wary of this rule. First, this does not obviate the requirements of a litigation hold (preserving evidence, suspending the provision of a document retention policy as needed, etc) – indeed, abiding by the litigation hold is part of the very definition of good faith. Moreover, though the court may not impose sanctions under these rules, nothing prohibits the court from imposing sanctions based on other rules, statutes or regulations and many commentators expect that they may do exactly that.

THE MEN IN BLACK SPEAK

We have had the opportunity to hear several federal judges speak about the new amendments recently. Judge T.S. Ellis III, from the Eastern District of Virginia, says candidly that he was opposed to the rules because he doesn’t believe amendments should be passed until the barbarians are at the gate. To his own surprise, he came to believe that the barbarians were indeed at the gate and dropped his opposition. He is pleased that the rules are modest in scope and largely incorporate electronic information into current practice. He is quick to note that lawyers who are unreasonable or do not act in good faith with respect to the new amendments will not like anything he has to say. He also notes that, even if he chooses not to sanction unreasonable or bad faith attorneys, the reputation they’ve established with him will remain in his memory banks. His words certainly didn’t seem to bode well for those who might not try wholeheartedly to comply with the new amendments.

Magistrate Judge Thomas Rawles Jones,, Jr., also from E.D.V.A. says he is concerned about the potential for abuse that the rules provide. Just as with paper, he is worried about lawyers who seem always to play the game of “hiding the ball.” He expressed a low tolerance for such behavior. He notes that “Litigation is the highest form of gambling and electronic evidence has upped the ante. Your job is to come to a reasonable resolution. It is a high stakes crap game to get involved in a lawsuit.” When asked how he would define “bad faith,” the judge noted simply “I know it when I see it.” A sidebar concern for Judge Jones is that litigious folks may try to “stick up” a corporation by filing a lawsuit where the electronic discovery would be so crippling and costly that the corporation might fold its cards and cave in to settlement rather than go through the pain. This problem, he says, will have to be sorted out on a case by case basis.

Magistrate Judge Michel Urbanski, from the Western District of Virginia, observed “this is hard stuff: all these changes reflect a generation gap. Many in the room (at a CLE) have not actually held a Bates stamper. These new rules are more a sea change for lawyers than judges – the lawyers’ duties have really changed much more than ours.” He also suggests that these rules cannot be read alone – that the comments to the rules are invaluable and will be used by judges to formulate their opinions because they contain a lot of background and “meat” not in the rules themselves.

Lastly, he predicts that “it will take a while to sort these rules out. Judges are here to help you. If you have problems, come talk to me and I’ll do my best to help.”

All three judges seemed to hold that opinion. So are you still scared? The basic message we heard from the men in black was to act ethically, reasonably and in good faith, bringing any concerns to them.

There’s your crib sheet, and in the immortal words of Sean Connery in *The Untouchables*, “Here endeth the lesson.”

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