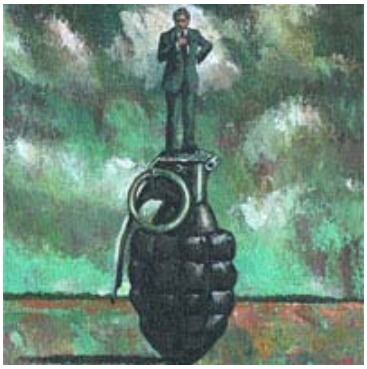
EDD Showcase: Worst Case Scenario

By Craig Ball

Send this to a colleague

Reprints & Permissions



If you engage in e-discovery, chances are you depend on vendors to help you harvest, process, search, and filter digital evidence. But is that a dependency that blurs the line between lawyer and service provider?

Selecting responsive information, planning search strategies, and deciding forms of production are responsibilities traditionally reserved to counsel. But confronted by the Gordian knot of EDD, lawyers now share — and sometimes surrender — aspects of that role to vendors and experts. When all goes well, delegation seems sensible. But what happens when a vendor error exposes lawyers to malpractice allegations, or clients to needless expense, sanctions, or even an adverse judgment? Several recent cases and incidents underscore the risks.

The American Lawyer recently reported that LexisNexis Applied Discovery Inc. used software that blanked the contents of older e-mail messages. Though LNAD assured customers that the problem affected only a minute fraction of its work, the company faces questions about quality assurance and its failure to timely apply software patches. (See Sept. LTN.)

Flawed search methods also contributed to the $1.45 billion dollar verdict in *Coleman (Parent) Holdings v. Morgan Stanley*, 2005 WL 679071 (Fla.Cir.Ct. March 1, 2005). And expert incompetence drew the judge's ire and sanctions in Gates Rubber Co. v. Bando Chem. Ind., Ltd., 167 F.R.D. 90 (D. Colo. 1996). On Dec. 1, 2006, new federal rules move EDD to center stage. For years to come, lawyers and EDD vendors will be joined at the hip in an uneasy alliance.

EDD Showcase: When Vendors Let You Down

Who is responsible when you delegate EDD and things go awry?

What should lawyers and firms do when faced with a serious vendor blunder? How can they protect their clients, and themselves? We turned for advice to three lawyers who work as electronic data discovery consultants:

- Michael Arkfeld, a Phoenix-based former assistant United States attorney, and a member of the LTN Editorial Advisory Board, is the author of Electronic Discovery & Evidence (Law Partner Publishing). E-mail: michael@arkfeld.com.

- Craig Ball, a certified computer forensic examiner and LTN columnist ("Ball in Your Court"), also serves as a court-appointed special master in electronic discovery. Based in Austin, his e-mail is craig@ball.net.

- J. William Speros, of Cleveland, is a former mainframe programmer, and focuses on litigation data management, and serves as a project manager and EDD dispute mediator. His e-mail is speros@speros.net.

Let's start the discussion with these questions:

Is law firm liability for EDD snafus on the rise?

Do we face the specter of billion dollar exposures no firm could weather? Is a lawyer vicariously liable for the omissions of the EDD vendor?

BALL: I'm fascinated by the Phoenix Four v. Strategic Resources Corp., 2006 WL 1409413 (SDNY Mary 23, 2006) decision, where a law firm was sanctioned along with the client for what, as I see it, amounts to a failure to ask the right questions about electronic evidence. The court called the lawyers' failure "gross negligence," and we all know where that leads.

Then, there's the Coleman (Parent) Holdings v. Morgan Stanley debacle where the judge excoriated defense counsel and revoked his pro hac vice (later reinstated on appeal). In a last ditch effort to dig out of a billion dollar hole, in-house counsel appears in open court and announces Morgan Stanley's intention to sue its lawyers for malpractice as a consequence of the EDD mess they were in. Ouch!

ARKFELD: In several cases, courts have considered sanctions for failure of the EDD vendor to timely process electronic data for disclosure to the opposing party. What is particularly telling is that the courts did not even discuss the lawyer and EDD vendor relationship, but assumed the lawyer would be sanctioned if the vendor did not perform in a timely manner.

In two cases, Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) and In re Worldcom, No.CIV.02-3288, 2004 WL 768573 (SDNY April 12, 2004), judges issued strongly-worded opinions that held under advisement possible imposition of sanctions — depending upon further discovery of the reasons for the processing delay, or if the vendor failed to process the data by a specific date.

SPEROS: If the attorney isn't responsible for managing evidence, who is? Isn't the lawyer who fails to assess and manage a vendor responsible for that vendor's bad acts — just like any other master liable for an agent's bad acts in the scope of employment? We've seen courts hold parties responsible for failing to supervise their vendors.

ARKFELD: Courts have been very active in directing lawyers to use EDD experts for such tasks as setting search protocols and certifying collection procedures. In fact, they have admonished counsel for failure to confer with experts re: EDD. But with the mandate to engage experts comes the obligation to select capable ones, or face sanctions and liability.

BALL: Wow! You guys are tough, but at least you're not saying it's strict liability. Some readers may wonder, is it really any different than a copy service losing a box of documents or a court reporter getting the testimony wrong?

I think that it is different. Those are the kinds of errors that lawyers are equipped to detect and rectify. We do paper very, very well. But EDD demands both special tools and technical expertise that most lawyers or firms simply don't possess.

Vendors tout proprietary processes and market their services like a big black box: Data goes in. Magic happens. Production comes out. How's a lawyer supposed to oversee that?

ARKFELD: One of the critical foundations of our civil justice system in America is the right to discover evidence to support your cause of action. From an ethical and legal perspective it is our duty to ensure that evidence is preserved and subsequently disclosed to the opposing party.

As a lawyer, if you chose to have an EDD vendor process and then search the data in response to disclosure obligations, the attorney must be reasonably confident that the processing and searching methodology is sound and that the evidence was disclosed and did not mysteriously disappear in a vendor's "black box."

Among the many things a vendor should do is to provide affidavits, testing data, etc., detailing how a particular piece of software processes electronically stored information (ESI). This may include hardware and software data to ensure accuracy in data processing, verification of procedures for entering data into the computer, auditing safeguards, the method of storing the data, and safety precautions to prevent data loss while in storage.

This would also apply to search software: lawyers must use reasonable care to ensure accuracy. Determine the idiosyncrasies of the search software? Does it perform straight Boolean or fuzzy searching, or use other techniques? Are testing certifications available? I always wonder how a lawyer would explain to the court that it was not his or her

fault. "The computer failed to find the responsive data" reminds me of the classic excuse, "My dog ate my homework."

BALL: I applaud Mike Arkfeld's emphasis on getting to the evidence. The needs of the requesting party sometimes get drowned out by the chorus of complaints about burden and cost. But as much as I share your aspiration, I question whether it's realistic or even fair to expect a lawyer to ensure the accuracy of search software. Wouldn't the lawyer have to hire a second expert to ride herd on the first?

ARKFELD: Not necessarily. A lawyer can evaluate software without understanding how it works — for example, by requiring the vendor to obtain an independent evaluation, asking other users about their experience, or by interviewing the vendor's employees who routinely use the program. No one knows the shortcomings of an application like those who use it all the time. The point is not to throw up your hands and assume you can't understand it. The goal is to be able to demonstrate that you didn't just accept marketing hype as true.

SPEROS: An attorney has a duty to manage a vendors' processing, even if the systems are proprietary and complex, and even if the attorney must do so through an expert. In the ESI context, attorneys must assign appropriately trained litigation support professionals, technology paralegals, or associates to oversee evidence management. These project managers must document their efforts, challenges, and results.

They should use checklists to guide the evidence management project plan, to meet new rules' requirements for early and extensive ESI identification and preservation. That checklist should include criteria to select vendors, based upon interviewing vendors' other clients.

BALL: Unfortunately, a common sense approach to due diligence is frequently overlooked. Too often, the only due diligence we see is price shopping.

SPEROS: Vendor selection can be hazardously casual — we've seen some chosen because they previously performed photocopy services and continue to deliver candy.

ARKFELD: I'd begin the process by aligning myself with quality EDD vendors who provide workflow certification affidavits, software processing, and accuracy test results — anything that would bear on the processing, searching, and filtering capabilities of any software used by the firm or EDD vendor and their workflow procedures. The bottom line is that when you handle electronic or paper evidence, you need to include quality control standards that assure disclosure of all responsive evidence to the opposing side. These efforts must be reasonable and documented. I suspect all trial attorneys have had to stand up before a judge and explain discovery problems, and hope for a favorable ruling. In my experience, the one thing judges insist on is that you take reasonable steps to diligently search, process, and disclose responsive discovery. Courts understand that we are in a transition from paper to EDD, but they are adamant that we use reasonable care in the selection of vendors or software. They will be enraged, and sanctions will follow, if you have not taken proper steps and then evidence is not disclosed.

BALL: What about indemnity agreements? My sense is that the big players in the EDD marketplace have their contracts, and it's something of a take-it-or-leave-it proposition, unless you're bringing them a multimillion-dollar project. Worse, contracts disclaim consequential damages, so companies holding themselves out as experts won't accept liability when they fail to deliver expertise.

SPEROS: I've tried to add indemnification clauses in e-processing vendors' contracts without much success. But, to be fair, I'm not surprised that vendors object to incurring boundless consequential damages to obtain service contracts that sometimes offer modest income.

Instead, I normally hire the vendor who will provide a white paper and sworn testimony and will take other reasonable steps requested by the client, including describing all tasks performed consistent with the project agreement.

I expect vendors to put it in writing and defend the quality of their work, but I don't expect them to indemnify. The buck stops with the party who bears the primary responsibility: the attorneys.

BALL: Where does the safe harbor provision of the new FRCP 37 fit into all this? Might a vendor's error fall under the umbrella of information lost due to a routine, good faith operation of an electronic information system?

ARKFELD: Over the last several weeks I have been surprised at the different interpretations this rule has been given by lawyers and commentators across the country. Some lawyers feel this is a "true safe harbor" and are advising their clients they don't have to worry about destruction or failure to preserve relevant evidence. They interpret the rule to mean that until the parties agree upon what data needs to be disclosed, there's no need to preserve. This interpretation flies in the face of the Committee Note:

"The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold."

"Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information. . . ."

As to service bureaus, the first issue is whether the rule applies to a vendor that processes data on behalf of one of the parties, which seems to be stretching the background history and intent of the rule. Assuming for the moment that it does apply, then did the vendor use good faith in processing the data. Good faith would surely involve what due diligence was exercised in the selection of software or vendors who process data on behalf of a party and what quality assurance steps the vendor had in place to ensure an accurate result.

SPEROS: I think the safe harbor relates to a client's inadvertent data loss prior to acquisition rather than attorneys' data loss after acquisition.

BALL: Though I also tend to take a restrictive view of the safe harbor rule, the vendor error situation is one where I'm sympathetic to its use to protect the lawyer and client from sanctions.

The rule doesn't say "information lost to routine, good faith operation until the lawyers get involved." If the information lost, or in the case of flawed search tools, the information not found, resulted from a legitimate oversight by a vendor whom the lawyer and client reasonably believed to be competent, I just don't see the rationale behind punishing the lawyer or client.

One of my favorite quotes from Justice Oliver Wendell Holmes is that, "Even a dog distinguishes between being stumbled over and being kicked." Punish the one who kicks, but only require the stumbler to make good on the damage.

SPEROS: Wouldn't Oliver Wendell Holmes' dog be entitled to bite the leg of the attorney who stumbled because the attorney declined to turn on a light? Attorneys are in the business of managing evidence they receive; I'd expect their standard of care to be more stringent than clients whose primary business is not preserving and acquiring evidence. Attorneys would be ill advised to look to the 37(f) safe harbor to protect lost evidence.

BALL: We will have to let sleeping dogs lie on Rule 37(f). But if the safe harbor doesn't protect clients and firms who are diligent in preservation, but lose data because it's entrusted to an errant expert, then the rule's a toothless mutt. As we say down my way, "That dog don't hunt." Instead, I'd expect the side that hired the vendor to reimburse the costs of repeated depositions, reprocessing data, follow-up searches and all other reasonable damages. I'd then expect them to secure reimbursement from the negligent vendor. Let's not forget that the prod- ucing party may be a victim here as well. The information lost could have helped either side. I'm just not ready to punish the lawyer or client absent some evidence of bad behavior.

Let's stand in the shoes of a lawyer who learns, two weeks before trial, that a programming error by the EDD vendor she persuaded her client to hire has resulted in the failure to search hundreds of thousands of e-mail messages that might hold responsive data.

The other side has taken a dozen depositions since the lawyer certified that all responsive e-mails were produced. What's the strategy?

SPEROS: A prudent attorney would fully disclose the problem to the other side even if its entire scope or implications were not yet known. At the same time, that attorney would fully advise the firm's malpractice insurance carrier.

Then that attorney would engage and supervise resources to fully investigate the problem all the while keeping the other side and the malpractice insurer apprised. Then, when the time is right, the firm could take action against the vendor to recover those costs — assuming the vendor's duties are spelled out in a meaningful contract. As you said earlier, Craig, sometimes the only business term considered and formalized is price.

BALL: I'd probably hold off on suing the vendor because I need their mea culpa in court, and they probably still have custody of my client's data. There will be time for finger-pointing later. Right now, I want to choose my battles and fight on one front. You can't overstate the importance of detailed, unvarnished disclosure. There's no need to fall on your sword (though saying, "We're sorry" can't hurt), but you must strive to recapture every shred of credibility you can.

If the court's livid — and so close to trial, that's almost a given — I'd seek appointment of an EDD special master at my client's sole cost. A special master will serve as a problem solver and a buffer against an angry judge. I'd tell the lawyer what I'd tell my kids: "Own up to the error. Don't make excuses. Try to make it right."

ARKFELD: I would immediately notify the opposing side and the court, as soon as I learn about it. Many of the decisions regarding sanctions focus on the reasonableness of lawyers' actions to preserve and process data. If the lawyer exercised reasonable due diligence in the selection of the vendor, I think the court will consider these circumstances in deciding whether to continue the trial date, reschedule depositions, and whether to impose sanctions. When problems like this occur, immediately take remedial action!

BALL: To wrap up our discussion, there is a bright side — much of the fear of sanctions and liability is unfounded.

Courts aren't handing down sanctions for diligent, good faith efforts gone awry.

To date, EDD sanctions have been almost invariably confined to cases of obstructive behavior and intentional destruction of evidence.

But we're all on notice now, especially as of December 1. Judges expect more from us with respect to electronically stored information.

The upshot is, lawyers must learn more about electronic evidence. We can't protect our clients from vendor error if we can't distinguish between good and bad EDD practices.

Law Technology News October 2006