

# **E-Discovery: Right...from the Start**

**Craig Ball**

**Right from the Start: 8 Ways to Hit the Ground Running**

**Selecting, Engaging and Working with E-Discovery Service Providers**

**Piecing Together the E-Discovery Plan: a Plaintiff's Guide to Meet and Confer**

## Right from the Start Smart First Steps in Electronic Discovery

Craig Ball  
© 2008

Certainly it's smart to prepare for e-discovery—to be “proactive” about electronically stored information (ESI) and implement early case assessment systems and strategies. But sometimes, the lawsuit's the first sign of trouble, and you have to choose which fires to fight...and fast.

Don't be paralyzed by fear of failure or confusion about where to begin. There are no perfect e-discovery efforts. Before the ESI experts come aboard, there are things you can and must do. Here's a quick compendium of eight ways to hit the ground running:

1. **Apply the five Ws of good journalism—who, what, when, where and why**—to get a handle on your core preservation duties. Immediately make a list of the people, events, time intervals, business units, records and communications central to the case.
  - a. List the apparent key players (don't forget assistants who, *e.g.*, handle the boss' email and significant third parties over whom your client has a right of direction or control).
  - b. Hone in on what happened—both from your perspective and theirs—and posit what ESI sheds light either way or tends to explain or challenge the key players' actions and attitudes.
  - c. Decide what dates and time periods are relevant for preservation. Is there a continuing preservation obligation going forward?
  - d. Determine which business units, facilities, systems and devices most likely hold relevant ESI.

Your lists will change over time, but a focused, thoughtful and well-documented effort, diligently implemented, is more defensible, less costly and invariably more effective than a scattershot approach. Don't delay. It needn't be flawless right now; reasonable will do.

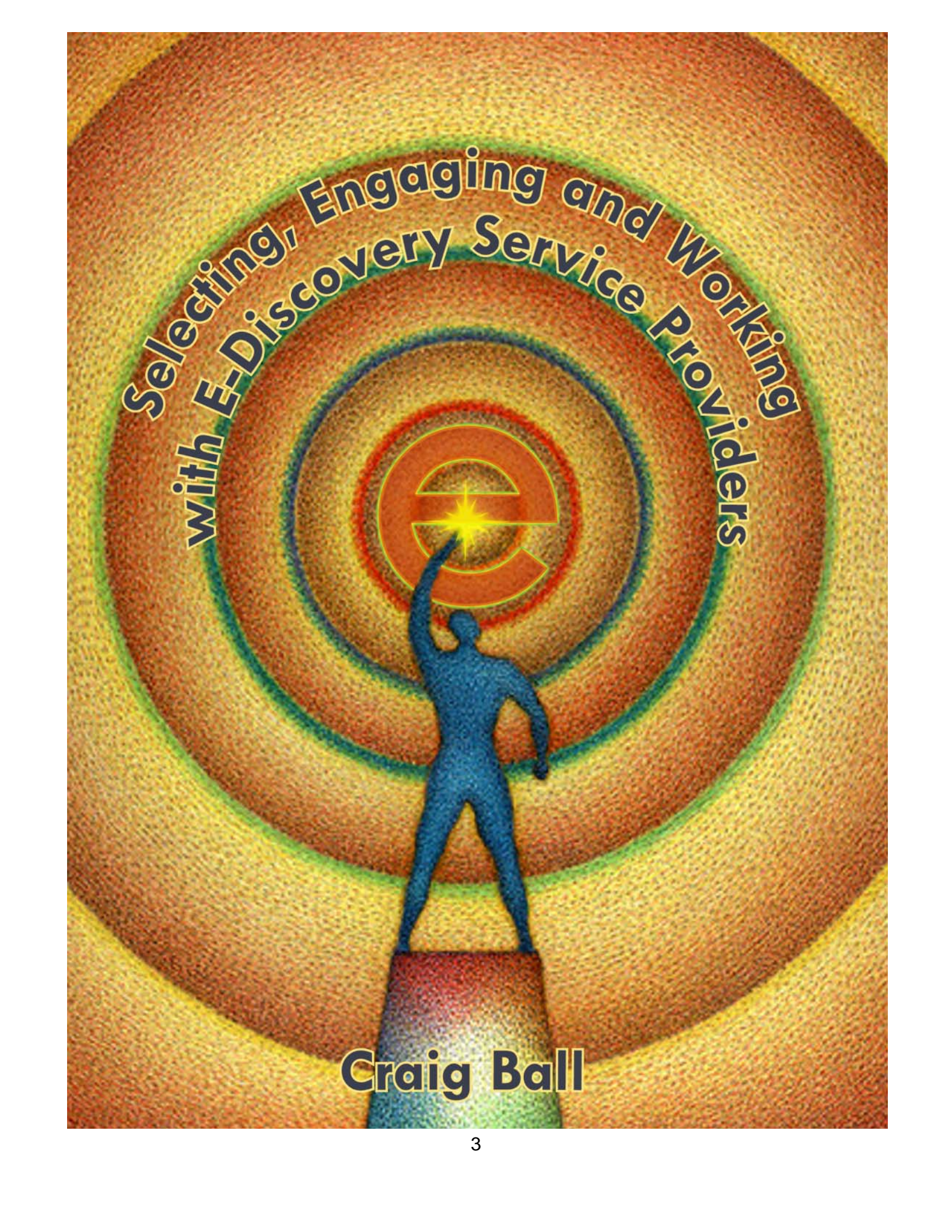
2. **Focus on the fragile first.** What potentially relevant ESI has the shortest shelf life and requires quickest action to preserve while it's still reasonably accessible? Voice mail, web mail and text messaging, computers requiring forensic examination, web content and surveillance video are examples of ESI that tend to be rapidly discarded or overwritten. Grabbing e-mail of key custodians *before* it migrates to backup media can save a bundle and accelerate search and processing.
3. **Protect employees from themselves.** People who wouldn't dream of shredding a paper record will purge ESI with nary a thought. In the blink of an eye, history will be reinvented as employees delete overly candid e-mail and commingled personal and business communications. The results are often catastrophic and always costly. Assess whether those entrusted with preservation can be trusted to perform, and don't rely on custodial preservation *alone* when its failure is reasonably foreseeable.

4. **Holds should be instructional, not merely aspirational.** Too many lawyers draft legal hold instructions designed to protect lawyers. Broadly disseminating a form hold directive saying “keep everything” isn’t helpful and will come back to haunt you at deposition. “I *got* that memo,” they say, “but I didn’t *do* anything.”

Custodians need to know where to start. Tell them what to do and how to do it. Give examples that inform and deadlines that demand action. Get management buy in for the time needed to comply. Better a handful of key players take the hold directive seriously than dozens or hundreds of minor players wink at it.

5. **Boots on the ground.** Good doctors don’t diagnose over the phone. Likewise, good lawyers meet key players and get a firsthand sense of how they operate. Seek out the people who manage the systems that hold the evidence, and learn the “who, what, when, where and why” of your client’s ESI face-to-face. It’s not just enormously helpful—it’s what courts demand.
6. **Build the data map, including local collections and databases.** Federal practice requires identification of potentially relevant ESI, but it’s a best practice everywhere. That goes for the less-accessible stuff, too. Courts won’t accept, “We don’t know what we have or where it is,” so be ready to identify potentially relevant ESI that you will and won’t explore or produce. Data stored off the servers or on databases pose special challenges made harder by turning a blind eye to its existence. Don’t fall prey to, “If we don’t tell them we have it, they won’t ask for it.”
7. **Consider how you’ll collect, store, search, review and produce ESI.** All ESI is just a bunch of ones and zeros. Making sense of it, controlling costs and minimizing frustrating “do-overs,” rides on how you choose to process and produce information. So add an “H”—*How*—to those five Ws, and ponder your options for how the data gets from here to there.
8. **Engage the other side.** Even warring nations cease fire to carry off fallen comrades. You don’t have to like or trust the opposition, but you have to be straight with them if you want to stay out of trouble in e-discovery. Tell the other side what you’re doing and what you’re unwilling to do. Collaborate anywhere you can. Lawyers over-discover cases more from ignorance and mistrust than guile or greed; but, even when you face someone gaming the system, your documented candor and good faith effort to cooperate will serve you well in court.



The background of the entire page is a textured, concentric circular pattern in shades of yellow, orange, and brown, resembling a target or a tunnel. In the center, a blue silhouette of a person stands on a narrow, multi-colored path that leads from the bottom towards the center. The person's right arm is raised, pointing towards a glowing yellow 'E' that is positioned at the center of the innermost circle. The 'E' is surrounded by a bright, starburst-like light. The text 'Selecting, Engaging and Working with E-Discovery Service Providers' is written in a bold, white, sans-serif font, following the curve of the upper part of the target pattern.

**Selecting, Engaging and Working  
with E-Discovery Service Providers**

**Craig Ball**



## Selecting, Engaging and Working with E-Discovery Service Providers

By Craig Ball<sup>1</sup>

The transmittal letter in the overnight package reads simply, “Enclosed please find Defendant’s production.” Peering in, you see a power supply, USB cable and external hard drive. “Finally,” you [sigh] [exult], “the documents we’ve been fighting to get.”

Eagerly connecting the drive to your computer, you browse its contents to find tens...wait...*hundreds* of thousands of cryptically named files in dozens of folders. Clicking at random prompts the computer to repeatedly ask what program you would like to use to open them. “*How should I know?*” you grumble. On the next click, the computer stops asking and launches your e-mail program. To your horror, you see that the defendant’s messages now fill your mailbox. “Uh oh,” you realize, “maybe I should have gotten some help with this.”

Increasingly, plaintiffs counsel succeed in discovering electronically stored information (ESI), but find they can’t handle what’s produced. Once, we might have dealt with a “document dump” by rolling up our sleeves and putting in extra hours; today, more time and effort are unavailing if you can’t search or even read the ESI.

For most plaintiffs’ counsel, the challenges of understanding and managing what’s been produced can be met only by enlisting the aid of an electronic discovery service provider.

Both sides must identify, preserve, cull and produce relevant ESI, and there’s no shortage of guidance published and sold to aid producing parties. The legal technology marketplace fairly teems with companies promising to help major law firms and corporate America get a grip on e-discovery. But, where do *you* turn for e-discovery services, and how do you protect yourself from paying too much or buying what you don’t need or won’t work? This article suggests strategies for the lawyer on the receiving end of an ESI production.

### **Know Your Needs**

Lawyers often head for the e-discovery marketplace lacking a clear picture of what they need. They buy the wrong services at the wrong price from unreliable providers and end up with little or nothing they can use.

The most effective steps you can take to insure success in your dealings with EDD service providers should occur *before* you start looking for help. You need to assess your case and do some preliminary research. Based on what you know of your opponent and the events at the heart of the claim, what types of electronic evidence are likely to exist, where and in whose custody does it reside, and what forms might it take? That’s not as hard as it sounds.

If your client is a current or former employee of the defendant, he or she can clue you into how the company managed information. If the defendant is a large corporation, there’s a good chance the Internet will yield insight into their information technology (IT) systems. A colleague who’s litigated against the defendant can help, as can a friend or associate with IT expertise, optimally--but not necessarily--in the same industry. IT systems have more similarities across

---

<sup>1</sup> The author gratefully acknowledges the contributions of colleagues Ann Marie Gibbs, Sharon Nelson, John Simek and Linda Richenderfer in generously sharing their time and insights.

companies than differences, so even someone without specific knowledge of the defendant's systems can help you master essential concepts and terminology.

### **Know your Current Capabilities**

Ideally, you specified the form of production for any ESI produced and received forms you know how to handle.<sup>2</sup> If not, you'll probably need help selecting and setting up ways to store, search, sort, review and annotate the production.

The right approach fits your practice and your budget. Help the service provider achieve that fit by being prepared to answer these questions about your capabilities:

- Where are we now in terms of computer and network hardware, applications owned and used, network bandwidth, storage capacity and in-house expertise and support?
- How do we currently use computers to manage voluminous production?
- How comfortable are we working with ESI?
- How much time can we devote to learning to use new tools?
- Considering the anticipated value of the suit, what is our budget for services, hardware and software?
- Should we invest in tools, hardware and training that we can use in more than one case?
- Can we share the cost or the work with other firms or parties in the case?

### **Know Your Goals**

Decide what capabilities you're seeking in a review platform<sup>3</sup> for particular tasks, For example:

While reviewing the other side's e-mail, I want to be able to:

- Use software and hardware I already own;
- Search the messages and attachments for words or phrases;
- Use proximity, fuzzy, Boolean and/or wild card search capabilities and stemming;

---

<sup>2</sup> FRCP Rule 34(b) contemplates that requesting parties will specify the form or forms of ESI production sought and that, absent objection or court order, production will be made in your specified form or forms. If a requesting party fails to specify a form or if a producing party objects to the requested form or forms, the producing party is obliged to state--in a written response filed within 30 days or at such other time as the parties agree to in writing or the Court directs--the form or forms in which it intends to make production. Absent a specification of form by the requesting party, the information must be produced in the form or forms in which it is ordinarily maintained or in a reasonably usable form or forms. FRCP Rule 34(b)(ii).

<sup>3</sup> "Review Platform" is the buzzword for the software, hardware and services used to store, display, sort, search, tag, code, annotate, redact and/or produce ESI. There are many review platforms on the market, including the familiar LexisNexis Concordance (<http://law.lexisnexis.com/concordance>) and CT Summation (<http://www.ctsummation.com/>) applications, Internet-accessible hosted review environments and proprietary "solutions" marketed by e-discovery service providers.

If your firm doesn't already own tools like Concordance or Summation that are well-suited to ESI review after some slicing and dicing of the data, consider whether powerful and low-cost desktop search tools like DT Search (<http://www.dtsearch.com/>) meet your search and retrieval needs. The tradeoff to using tools not designed for e-discovery is that they lack key work flow features like document annotation, deduplication, issue coding and metadata management. Unfortunately, the solo and small firm e-discovery market hasn't stirred sufficient interest among developers for the emergence of a right-sized and right-priced desktop review suite adapted to day-to-day litigation. However, there's a fast-growing market for an e-discovery application akin to what QuickBooks offers for small business accounting. Either an affordable EDD tool kit will emerge or the cost of online storage and review services will drop to fill the void.

- View routine attachments on the fly;
- Deduplicate more than a single instance of identical or nearly identical items;
- Collaborate with other reviewers on my team;
- Attach notes or categorize the messages in my own way; and/or
- Expose relationships among senders and recipients or automatically find similar items.

Small efficiencies gained for each item reviewed pay handsome dividends applied to thousands of items. Also, stay mindful of how you plan to authenticate, use and present ESI at deposition or in trial.

### **The E-Discovery Marketplace**

Have you ever gone to the grocery store without a list and bought things you really didn't need? If so, you'll appreciate the economy that comes from deciding what you want before approaching vendors. Certainly, you need to listen, but don't let a salesperson talk you into products or services you neither want nor fully understand. When you cut through the marketing hype, you'll find that vendors provide similar services. Differentiation arises from experience, price, support and the ability to scale to projects of varying size and complexity.

Are you seeking a consultant, processor, application service provider or software vendor? Consultants plan the work, processors do it, application service providers rent workspace and tools and software vendors sell them.

More specifically, **consultants** advise you on proper, cost-effective ways to preserve, collect, search, produce, seek and manage ESI. They help you target your discovery requests, distinguish meritorious objections from obstructionist tactics and specify forms of production. They'll evaluate vendors and bids and support you at meetings and conferences concerning ESI issues. Depending on expertise, they may also conduct computer forensic examinations, assess the accuracy and completeness of production or testify in court to defend or challenge the handling or production of the electronic evidence.

**Processors** collect ESI or convert it to preferred forms, often filtering specific content according to the needs of the case or creating indices and databases to help manage the information. You'll turn to processors when you need native e-mail or electronic documents converted to page images, text extracted from those images, paper scanned to searchable electronic formats and backup tapes restored. Processors also generate the load files holding metadata and text that must accompany TIFF page images in order for them to be searchable.

**Application service providers** (ASPs) host large volumes of ESI, making it accessible to you via secure network or Internet access, typically paired with online tools to aid searching, viewing, analyzing, annotating and categorizing the data. ASPs facilitate sharing information and allocating review tasks among litigation team members in different firms and locations. ASPs are sometimes called SaaS providers, for *Software as a Service*.

**Software vendors** sell programs that collect, archive, search, display, index, analyze, annotate, categorize and convert ESI. Software tools may be highly specialized, like those that track litigation hold efforts, or require extensive training, like those used for computer forensic analysis. Additionally, they may necessitate investment in dedicated hardware and data storage.

**E-discovery companies** fall into one or more of these categories, and full service providers typically consult on projects as well as process and host data. The boundaries aren't always clear cut; but as a rule of thumb, you'll pay the most for full service providers and the least for processors specializing in particular tasks, like restoration of backup tapes.<sup>4</sup> Of course, a processor is no bargain if you've bought the wrong service or don't know how to use what they deliver.

Hosting data with an application service provider is a good choice when collaborating with lawyers in different firms or locations. Because you pay every month, hosting with an ASP can cost more than alternatives when a case takes longer to resolve than anticipated. Though expensive, hosting eliminates much of the investment required to purchase software and develop in-house systems and, unlike capital investments, hosting costs can generally be passed on as cases expenses.

### **The Top Tier**

Legal magazines and websites are filled with ads for national e-discovery service providers promoting their expertise and "solutions." These vendors vie for attention at CLE conferences and trade expos, sponsor webcasts, fill mailboxes with glossy solicitations and compete aggressively for their slice of the multibillion dollar e-discovery pie.

You'd think they'd welcome your business; but for the most part, they don't want anything to do with you.

The top tier e-discovery service providers are geared to serve Fortune 500 corporations and the clients of large law firms. Their bread is buttered by enterprise-wide collection efforts, processing of huge volumes of data and the sale of sophisticated review and "early assessment" tools used by platoons of reviewers. Their business model hinges on developing relationships with customers for whom being sued or responding to government document requests is recurrent or routine. Even those who want your business may decline for fear of creating a future conflict in their target market.

Notable exceptions are plaintiffs' firms and litigation groups handling class action suits where the frequency and complexity of discovery efforts, as well as available funding, render them as attractive as large corporate clients. But for the plaintiffs' attorney looking for a hand with a few disks received in production or wielding the sling in David vs. Goliath discovery, the options are more limited and local.

### **Going Local**

The best way to find a good e-discovery vendor is to seek recommendations from other lawyers. Be sure to ask if they have firsthand knowledge of the vendor, what type of work was done and when. Check with colleagues who've spoken or published about electronic discovery at CLE

---

<sup>4</sup> Restoration of backup tape is a task where it particularly pays to work with a specialist. Only a handful of vendors are equipped to process tape in volumes that allow for economies of scale and fast turnaround. While the author doesn't endorse any vendor, the leading national specialists in backup tape restoration are eMag Solutions, LLC, based in Atlanta, GA; National Data Conversion, Inc., based in New York, NY; and Renew Data Corp., based in Austin, TX.



conferences. Those top tier companies who don't want your business can help in directing you to providers in or near your community who will be glad to have you as a customer.

Even communities too small to support a local e-discovery service provider may be home to a computer forensic examiner. It may be economically feasible to use a forensicist to process modest data volumes (e.g., collections from fewer than ten machines or under 500 gigabytes in aggregate post-processed production); but, the higher hourly rates of computer forensic examiners (\$150-500/hour) compared to those of e-discovery data processors may price them out of the job. Still, a local examiner should be sufficiently plugged into the e-discovery market in your region to suggest well-qualified vendors.

Searching the Internet for local leads can be frustrating. National providers tend to dominate responses, in part because search engines sell search terms and enhanced placement. Accordingly, you can't rely on responses reflecting the names of local service providers, even when you include the name of your community or a nearby city in your search.

### **Do Your Homework**

Anyone can have a flashy web presence, so be wary of companies with web sites thin on content or that shed little light on the experience and qualifications of the principals.

The lure of e-discovery dollars has prompted everyone from copy and scanning services to computers and network service technicians to offer e-discovery services. While some comelately vendors do fine work, it's difficult to know which local providers are reliable and which are merely trying to jump on the bandwagon. Don't hesitate to ask how long the vendor has been in business and offered e-discovery services. Ask what software packages they employ. Behind-the-scenes, many local providers employ the same off-the-shelf tools for e-discovery, and it pays to know if they are limited by their tools or possess the technical expertise to adapt to your needs.

Visit a processor's workplace. Is it orderly and up-to-date? Is it secure? Is it dedicated to e-discovery work or is e-discovery just a sideline? Especially in smaller communities, computer resellers or copy services may be trying to make ends meet by adding e-discovery to their repertoire; but if they don't do enough of it, they may not have the experience needed to perform.

Salespeople make plenty of promises, but they're rarely the ones who must deliver the goods. The quality of an e-discovery effort is closely tied to the skills and experience of the project manager. So find out who will be responsible for your project and get a handle on their accessibility and resourcefulness. Since you probably can't gauge those qualities in a brief meeting, ask for the names of recent customer references *and call them*. True, you won't get the horror stories, but even happy customers can open your eyes to problems. Always ask if the company met deadlines and budget projections.

Especially for local service providers, a call to the Better Business Bureau, a quick check for lawsuits and even purchasing a financial report can head off headaches. Any industry has its fly-by-nights and fools, ask around.

Don't forget to explore any conflicts of interest that may exist. You need to know if the vendor works for your opposing counsel or the defendant. You should also assess the vendor's ability to secure the premises and the data, particularly if produced subject to protective order or paired with your confidential work product.

You may also want a frank discussion about who pays for rectifying processing errors. Such errors occur with enough regularity that it's not a question of *if* they will happen but *when*. Companies that value their reputations won't hesitate to step up and fix their mistakes. Any hemming or hawing about this should give pause.

Finally, if the vendor will be conducting searches of the data on your behalf, it's imperative to establish their search capabilities and limitations. Do they support Boolean searches? Can they effectively search foreign language data employing multibyte encoding or "Unicode?" Do they offer enhanced search technologies like concept searching or visual analytics? Will they charge for "machine time" while searches are made?

### **Getting Started**

Whether a vendor charges by the page, the gigabyte or the hour, costs tend to rise with the volume of information processed and its complexity. Uncertainty leads to price padding, so one of the first steps a processor should undertake is to inventory the data. They need to know how many discrete files have been produced, their format and size. Nested files that contain other files (e.g., compressed archives and e-mail containers) can seriously skew volume and cost estimates, so you want to flag them and inventory their contents early. This is an opportune time to ensure that the vendor's systems are capable of recursing through nested data as deeply as required to extract all content and of identifying and interpreting all of the various file types produced.

Your next goal should be filtering to cull irrelevant data and deduplication to insure that you don't waste time looking at the same material over and over again. These efforts should incorporate ways to uniquely identify production items (if not already Bates stamped) and insure that the review doesn't impact the integrity of the electronic evidence. A technique called file hashing<sup>5</sup> is especially useful for this.

At this point, the vendor should be able to offer very reliable projections of the total cost to convert the data to more accessible forms. Be wary of cost projections based on "presumed" or "rule of thumb" page equivalencies. These are rarely accurate and tend to inflate the cost significantly. It's a good time to inquire about your exposure to "exception handling" charges--sums assessed when vendors must e.g., deal with oddball file types or decrypt password protected data.

### **V as in Victory...and Vendor**

The too-candid e-mail. The *res gestae* voice message. The purloined PowerPoint. More-and-more, the most compelling documents in your cases are digital. Lawyers able to discover, navigate and present electronic evidence hold the winning hand against those who

---

<sup>5</sup> Hashing is the use of an algorithm to calculate a distinctive alphanumeric value called a "hash" that ably serves as an electronic fingerprint for any digital data. Hashing supports unique identification and easy authentication of digital evidence. Common hash algorithms are MD5 and SHA-1. MD5 hash fingerprints are so unique that the likelihood of two differing files having the same hash value is estimated to be *one in 340 trillion trillion trillion*.

cannot, and the strength of that hand owes a lot to good working relationships with skilled, reliable e-discovery service providers.

Good help is hard to find—and some vendors you'll want to avoid--but with the right ESI expertise on your trial team, you'll be better able to unearth the buried bits and bytes, debunk the excuses and—just maybe--bring about that amazing alchemy of turning leaden production into golden justice.

## **21 Tips for Working with E-Discovery Service Providers**

1. Bone up on e-discovery before you wade in.
2. Find out all you can about the forms and volumes of ESI before approaching vendors.
3. Know what systems and software you already own capable of reviewing ESI.
4. Don't purchase products or services you or your staff don't know how to use unless you budget the time and money needed for training.
5. Visit the processing facility. Does it look like the photos on the website? Is it orderly and up-to-date? Is it secure?
6. Explore conflicts. You may not mind that the vendor is also working for the defendant or opposing counsel in other matters, but you need to know about it.
7. Establish the vendor's ability and willingness to deliver both the technical and testimonial support you'll need.
8. Insist on meeting the project manager or consultant who'll be assigned to your project. Is it a good fit? Can she communicate in non-technical language? Does she look shell shocked?
9. Get the cell phone numbers of your project manager and at least one other person working with your data.
10. Get customer references and talk with them. Did the vendor meet deadlines? How much work had to be reprocessed due to errors? Did actual charges significantly exceed projections?
11. It's a vendor's job to be certain you understand the scope of work, the reasons behind actions and what it will all cost. Don't be baffled by jargon or concerned about looking foolish. The only dumb questions are the one you don't ask.
12. Clearly establish the scope of work in writing, and be sure you understand all price components and how they are calculated.
13. For pricing based on data volumes, be certain you understand how volumes are calculated. Are bills based on raw volumes or determined after filtering? Beware of "page equivalency" calculations.
14. Guard against sticker shock by setting a threshold above which you must expressly authorize further work.
15. Even the sharpest attorneys can't find loopholes in the laws of physics. Large ESI volumes take time to duplicate, index, search and process, so be sure you allow sufficient time; else, be prepared to pay expedited rates and seek extensions.
16. Clearly communicate deadlines, and get written commitments to meet them.
17. Protect your ability to efficiently and economically recover your data if serious problems occur. Insure your data can't be "held hostage" in billing disputes.
18. Be sure you know what tasks the vendor handles in-house and what they outsource. Outsourcing may be smart, but you need to know why and what markups apply.
19. Arrange for your side's EDD technician to talk directly to your opponent's EDD technician. Their ability to speak the same language streamlines data transfer and establishes appropriate expectations.
20. The demand for talented e-discovery product managers far outstrips the supply, so there's a lot of turnover. Get acquainted with others working on your project before your project manager moves on. When crunch time comes, you don't want to hear, "She's gone, let me find out who's handling that now."
21. Don't wait until you need an e-discovery service provider to start lining up prospects. The need will be there. Having someone on deck helps you hit the ground running.



# Piecing Together the E-Discovery Plan: A Plaintiff's Guide to Meet and Confer



**Craig Ball**

## Piecing Together the E-Discovery Plan: *a Plaintiff's Guide to Meet and Confer*

By Craig Ball  
© 2008

*E-discovery is challenging, but it needn't be complicated by a battle-zone mentality. Take advantage of the meet-and-confer process to ensure that your opponents know what electronically stored information they have and how they should produce it.*

Everyone wants e-discovery to be simple. The defendant's tech guru wants it to be simple because he's got too much to do. The defendant's in-house counsel wants it to be simple because she's got budget issues and thinks most claims are frivolous. Outside counsel wants it to be simple because he likes doing things the way he's always done them and doesn't like looking clueless about electronic information.

And you want it to be simple because you need it to be simple. Hiring experts and e-discovery vendors raises the stakes, and a misstep may result in significant cost-shifting to your client. Moreover, if you don't ask the right questions, you're not going to get the right information--and aren't courts starting to sanction lawyers for e-discovery foul-ups?

The problem is e-discovery is not simple. It's complex, technical and tricky. There are no shortcuts--no form, checklist, or script that's going to get the defendant to find the relevant information and turn it over in a reasonably usable way.

Face it: you've got to *fight* to get electronic evidence. You have to know what they've got, what you need and how to ask for it. You must understand the capabilities and limitations of electronic search and the forms of production best suited to the evidence.

### **Meet and Confer**

In 2006, Federal Rule of Civil Procedure 26(f) was amended to require parties to confer about preserving discoverable information and to develop a proposed discovery plan addressing discovery of electronically stored information (ESI) and the form or forms in which it should be produced. The amended rule requires parties to confer about preserving discoverable information and to develop a proposed discovery plan addressing, *inter alia*, discovery of electronically stored information (ESI) and the form or forms in which it should be produced. This conference<sup>6</sup>, and the overall exchange of information about electronic discovery, is called "meet and confer."<sup>7</sup>

---

<sup>6</sup> The Fed. R. Civ. P. 26(f) conference must occur "as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b)...."

<sup>7</sup> *Hopson v. Mayor of Baltimore*, 232 F.R.D. 228, 245 (D. Md. 2006) details some of counsel's duties under Fed. R. Civ. P. 26(f):

"[C]ounsel have a duty to take the initiative in meeting and conferring to plan for appropriate discovery of electronically stored information at the commencement of any case in which electronic records will be sought....At a minimum, they should discuss: the type of information technology systems in use and the persons most knowledgeable in their operation; preservation of electronically stored information that may be relevant to the

The states are rapidly adopting rules of procedure and local practice like the Rule 26(f) meet and confer;<sup>8</sup> but even where no such rule exists, state judges often find the federal e-discovery model instructive and grant motions to compel parties to confer on ESI issues.<sup>9</sup>

## Sizing Up The Opposition

---

litigation; the scope of the electronic records sought (i.e. e-mail, voice mail, archived data, back-up or disaster recovery data, laptops, personal computers, PDA's, deleted data) the format in which production will occur (will records be produced in "native" or searchable format, or image only; is metadata sought); whether the requesting party seeks to conduct any testing or sampling of the producing party's IT system; the burdens and expenses that the producing party will face based on the Rule 26(b)(2) factors, and how they may be reduced (i.e. limiting the time period for which discovery is sought, limiting the amount of hours the producing party must spend searching, compiling and reviewing electronic records, using sampling to search, rather than searching all records, shifting to the producing party some of the production costs); the amount of pre-production privilege review that is reasonable for the producing party to undertake, and measures to preserve post-production assertion of privilege within a reasonable time; and any protective orders or confidentiality orders that should be in place regarding who may have access to information that is produced."

<sup>8</sup> Noted e-discovery commentator Thomas Allman, a founding member of the Sedona Conference and co-chair the E-Discovery Committee of the Lawyers for Civil Justice, reports that seven states that have adopted e-discovery rules hewing closely to the Fed. R. Civ. P. (Louisiana, Minnesota, Montana, New Jersey, Utah, Arizona and Indiana). Allman notes another 14 states are considering changes to their court rules to address e-discovery (Alaska, Connecticut, Florida, Illinois, Iowa, Kansas, Maryland, Nebraska, New Mexico, North Dakota, Ohio, Tennessee, Virginia and Washington). See Brett Burney, *Mining E-Discovery Stateside*, Law Technology News (January 18, 2008).

<sup>9</sup> See, e.g., Conference of Chief Justices, *Guidelines For State Trial Courts Regarding Discovery Of Electronically-Stored Information*, Section 3 (2006), stating that a judge should "encourage" counsel to meet and confer in an effort to agree on e-discovery issues and to exchange information, *inter alia*:

- (1) A list of the person(s) most knowledgeable about the relevant computer system(s) or network(s), the storage and retrieval of electronically-stored information, and the backup, archiving, retention, and routine destruction of electronically-stored information, together with pertinent contact information and a brief description of each person's responsibilities;
- (2) A list of the most likely custodian(s), other than the party, of relevant electronic data, together with pertinent contact information, a brief description of each custodian's responsibilities, and a description of the electronically-stored information in each custodian's possession, custody, or control;
- (3) A list of each electronic system that may contain relevant electronically-stored information and each potentially relevant electronic system that was operating during the time periods relevant to the matters in dispute, together with a general description of each system;
- (4) An indication whether relevant electronically-stored information may be of limited accessibility or duration of existence (e.g., because they are stored on media, systems, or formats no longer in use, because it is subject to destruction in the routine course of business, or because retrieval may be very costly);
- (5) A list of relevant electronically-stored information that has been stored offsite or off-system;
- (6) A description of any efforts undertaken, to date, to preserve relevant electronically-stored information, including any suspension of regular document destruction, removal of computer media with relevant information from its operational environment and placing it in secure storage for access during litigation, or the making of forensic image back-ups of such computer media;
- (7) The form of production preferred by the party; and
- (8) Notice of any known problems reasonably anticipated to arise in connection with compliance with e-discovery requests, including any limitations on search efforts considered to be burdensome or oppressive or unreasonably expensive, the need for any shifting or allocation of costs, the identification of potentially relevant data that is likely to be destroyed or altered in the normal course of operations or pursuant to the party's document retention policy.

Opponents weaned on a scorched earth, “take no prisoners” approach to litigation aren’t adapting well to the requisite openness and collaboration of meet and confer. They won’t tell you how they identified and collected responsive data. They’ll refuse to share custodial questionnaires or disclose keywords and filtering mechanisms. Deal with them by making your record and seeking the court’s intervention. Angry judges, sanctions and unhappy clients are the Darwinian factors bringing about the extinction of Obstructasaurus Lex.

Obstructive opponents aren’t your only obstacle. Well-intentioned producing parties present challenges, too, and tend to split into three camps:

**Those who accept the duty to preserve and produce ESI, want to do it right, but don’t know how:** These opponents are ill-equipped to guide preservation or ask the right questions. Here, be prepared to fill the knowledge gap in a non-threatening manner—a daunting challenge in a profession where few are willing to admit weakness—or find ways to convince your opponent to get expert help. Bringing your own expert to conferences or hearings helps the other side see they are in over their heads.

**Those who accept the duty, but know only one way to deal with ESI:** These opponents have settled on an approach that worked for them in another case and are determined to employ it in every case. Their method might entail, e.g., over-reliance on custodial collection or a blind devotion to TIFF image production, even when it destroys the integrity of the evidence. Here, you need to understand their approach and determine if it’s going to work. If not, be prepared to demonstrate where it falls short and offer suitable alternatives. The right solution may be a *hybrid* production integrating alternative techniques for categories of ESI that don’t lend themselves to the other side’s approach.

**Those who accept the duty, want to do it right and know how:** Here, the onus is on you to meet them on the level playing field, so know what you need and be prepared to settle on reasonable and effective methods to identify, preserve, select and produce the information without undue burden or cost. Be ready, and be reasonable.

### Preparing for Meet and Confer

E-discovery duties are reciprocal. Just because your client has little electronic evidence, you must nonetheless act to preserve and produce it. At meet and confer, be prepared to answer many of the same questions you’ll pose.

Meet and confer is more a process than an event. Lay the foundation for a productive process by communicating your expectations. Send a letter to opposing counsel a week or two prior to each conference identifying the issues you expect to cover and sharing the questions you plan to ask. If you want client, technical or vendor representatives in attendance, say so. If you’re bringing a technical or vendor representative, tell them. Give a heads up on the load file specification you want used or keywords you want searched, if only to let the other side know you’ve done your homework. True, your requests may be ignored or even ridiculed, but it’s not an empty exercise. A cardinal

*A cardinal rule for electronic discovery is to tell your opponents what you seek, plainly and clearly. They may show up empty-handed, but not because you failed to set the agenda.*



rule for electronic discovery, indeed for any discovery, is to tell your opponent what you seek, plainly and clearly. They may show up empty-handed, but not because you failed to set the agenda.

The early, extensive attention to electronic evidence may nonplus lawyers accustomed to the pace of paper discovery. Electronic records are ubiquitous. They're more dynamic and perishable than their paper counterparts, require special tools and techniques to locate and process and implicate daunting volumes and multifarious formats. These differences necessitate immediate action and unfamiliar costs. Courts judge harshly those who shirk their electronic evidence obligations.

### **Questions for Meet and Confer**

The following exemplar questions address the types and varieties of matters discussed at meet and confer. They're neither exhaustive nor tailored to the unique issues in your case. They're offered as talking points to stimulate discussion, not as a rigid agenda and certainly not as a form for discovery.

#### **1. What's the case about?**

Relevance remains the polestar for discovery, no matter what form the evidence takes. The scope of preservation and production should reflect both claims *and* defenses. Pleadings only convey so much. Be sure the other side understands your theory of the case and the issues you believe guide their retention and search.

#### **2. Who are the key players?**

Cases are still about *people* and what they did or didn't say or do. Though there may be shared repositories and databases to discover, begin your quest for ESI by identifying the people whose conduct is at issue. These *key players* are *custodians* of ESI, so determine what devices and applications they use and target their relevant documents, application data and electronic communications. Determine whether assistants or secretaries served as proxies for key players in handling e-mail or other ESI.

Like so much in e-discovery, identification of key players should be a collaborative process, with the parties sharing the information needed for informed choices.

#### **3. What events and intervals are relevant?**

The sheer volume of ESI necessitates seeking sensible ways to isolate relevant information. Because the creation, modification, and access dates of electronic documents tend to be tracked, focusing on time periods and particular events helps identify relevant ESI, but only if you understand what the dates signify and when you can or can't rely on them. When a document was created doesn't necessarily equate to when it was written, nor does "accessed" always mean "used." For ESI, the "last modified" date tends to be the most reliable.

#### **4. When do preservation duties begin and end?**

The parties should seek common ground concerning when the preservation duty attached and whether there is a preservation duty going forward. The preservation obligation generally begins with an expectation of litigation, but the facts and issues dictate if there is a going forward obligation. Sometimes, events like plant explosions or corporate implosions define the endpoint for preservation, whereas a continuing tort or loss may require periodic preservation for

months or years after the suit is filed. Even when a defendant's preservation duty is fixed, a claimant's ongoing damages may necessitate ongoing preservation.

#### **5. What data are at greatest risk of alteration or destruction?**

ESI is both tenacious and fragile. It's hard to obliterate but easy to corrupt. Once lost or corrupted, ESI can be very costly or impossible to reconstruct. Focus first on fragile data, like backup tape slated for reuse or e-mail subject to automatic deletion, and insure its preservation. Address back up tape rotation intervals, disposal of legacy systems (e.g., obsolete systems headed for the junk heap), and re-tasking of machines associated with new and departing employees or replacement of aging hardware.

#### **6. What steps have been or will be taken to preserve ESI?**

Sadly, there are dinosaurs extant who believe all they have to reveal about ESI preservation is, "We're doing what the law and the Rules require." But that's a risky tack, courting spoliation liability by denying you an opportunity to address problems before irreparable loss. More enlightened opponents see that reasonable disclosures that don't prompt objections serve to insulate them from sanctions for preservation errors.

#### **7. What nonparties hold information that must be preserved?**

ESI may reside with former employees, attorneys, agents, accountants, outside directors, Internet service providers, contractors, application service providers, family members and other nonparties. Some may retain copies of information discarded by your opponent. Absent your reminder, the other side may focus on their own data stores and fail to take steps to preserve data held by others over whom that have some right of direction or control.

#### **9. What data require forensically sound preservation?**

"Forensically sound" preservation of electronic media preserves, in a reliable and authenticable manner, an exact copy of all active and residual data, including remnants of deleted data residing in unallocated clusters and slack space. When there are issues of data loss, destruction, alteration or theft, or when a computer is an instrumentality of loss or injury, computer forensics and attendant specialized preservation techniques are required. Though skilled forensic examination is expensive, off-site, forensically-sound preservation can cost less than \$500 per system. So talk about the need for such efforts, and if your opponent won't undertake them, consider whether you should force forensic preservation, even if you bear the cost.

#### **10. What metadata are relevant, and how will it be preserved, extracted and produced?**

Metadata is evidence, typically stored electronically, that describes the characteristics, origins, usage and validity of other electronic evidence. There are all kinds of metadata found in various places in different forms. Some is supplied by the user, and some is created by the system. Some is crucial evidence, and some is just digital clutter. You will never face the question of whether a file has metadata—all active files do. Instead, the issues are what *kinds* of metadata exist, *where* it resides and whether it's potentially *relevant* such that it must be preserved and produced. Understanding the difference--knowing what metadata exists and what evidentiary significance it holds--is an essential skill for attorneys dealing with electronic discovery.

The most important distinction is between *application metadata* and *system metadata*. The former is used by an application like Microsoft Word to embed tracked changes and commentary. Unless redacted, this data accompanies native production (that is, production in the form in which a file was created, used and stored by its associated application); but for imaged production, you'll need to insure that application metadata is made visible before imaging.

System metadata is information like a file's name, size, location, and modification date that a computer's file system uses to track and deploy stored data. Unlike application metadata, computers store system metadata outside the file. It's information essential to searching and sorting voluminous data and therefore it should be routinely preserved and produced.

Try to get your opponent to agree on the metadata fields to be preserved and produced, and be sure your opponent understands the ways in which improper examination and collection methods corrupt metadata values. Also discuss how the parties will approach the redaction of metadata holding privileged content.

### **11. What are the defendant's data retention policies and practices?**

A retention policy might fairly be called a destruction plan, and there's always a gap—sometimes a chasm—between an ESI retention policy and reality. The more onerous the policy, the greater ingenuity employees bring to its evasion to hang on to their e-mail and documents. Consequently, you can't trust a statement that ESI doesn't exist simply because a policy says it *should* be gone.

Telling examples are e-mail and back up tapes. When a corporate e-mail system imposes an onerous purge policy, employees find ways to store messages on, e.g., local hard drives, thumb drives and personal accounts. Gone from the e-mail server rarely means gone for good. Moreover, even companies that are diligent about rotating their backup tapes and that regularly overwrite old contents with new may retain complete sets of backup tapes at regular intervals. They also fail to discard obsolete tape formats when they adopt newer formats.

To meet their discovery obligations, the defendant may need to modify or suspend certain data retention practices. Discuss what they are doing and whether they will, as needed, agree to pull tapes from rotation or modify purge settings.

### **12. Are there legacy systems to be addressed?**

Like legacy back up tapes, old computers and servers tend to stick around even if they've fallen off the defendant's radar. You should discuss whether potentially relevant legacy systems exist and how they will be identified and processed. Likewise, you may need to address what happens when a key custodian departs. Will the system be re-assigned, and if so, what steps will be taken to preserve potentially relevant ESI?

### **13. What are the current and prior e-mail applications?**

E-mail systems are Grand Central Station for ESI. Understanding an opponent's current e-mail system and other systems used in the relevant past is key to understanding where evidence resides and how it can be identified and preserved. Corporate e-mail systems tend to split between the predominant Microsoft Exchange Server software tied to the Microsoft Outlook e-mail client on user's machines and Lotus' Domino mail server accessed by the Lotus Notes e-

mail client application. A changeover from an old system to a new system, or even from an old e-mail client to a new one, can result in a large volume of “orphaned” e-mail an opponent may fail to search.

#### **14. Are personal e-mail accounts and computer systems involved?**

Those who work from home, out on the road or from abroad may use personal e-mail accounts for business or store relevant ESI on their home or laptop machines. Parties should address the potential for relevant ESI to reside on personal and portable machines and agree upon steps to be taken to preserve and produce that data.

#### **15. What electronic formats are common and in what anticipated volumes?**

Making the right choices about how to preserve, search, produce and review ESI depends upon the forms and volume of data. Producing a Word document as a TIFF image may be acceptable where producing a native voice mail format as a TIFF is inconceivable. It’s difficult to designate suitable forms for production of ESI when you don’t know its native forms. Moreover, the tool you’ll employ to review millions of e-mails is likely much different than the tool you’ll use for thousands. If your opponent has no idea how much data they have or the forms it takes, encourage or compel them to use sampling of representative custodians to perform a “data biopsy” and gain insight into their collection.

#### **16. How will we handle voice mail, instant messaging and other challenging ESI?**

Producing parties routinely ignore short-lived electronic evidence like voice mail and instant messaging by acting too late to preserve it or deciding that the retention burden outweighs any benefit. Though it’s not especially challenging to preserve voice mail or IM logs if one acts swiftly, defendants tend to demand a particularized need before they’ll do so. *When it’s relevant*, will the other side archive voice mail messages or activate local logging or packet capture of IM traffic?

#### **17. What relevant databases exist and how will their contents be discovered?**

From R&D to HR and from finance to the factory floor, businesses run on databases. When they hold relevant evidence, you’ll need to know the platform (e.g., SQL, Oracle, SAP, Documentum) and how the data’s structured before proposing sensible ways to preserve and produce it. Options include running agreed queries, exporting relevant data to standard formats like Access databases or XML or even mirroring the entire contents to a review environment.

Because databases are always changing, Michael Arkfeld, author of the respected treatise “Arkfeld on Electronic Discovery and Evidence”<sup>10</sup> cautions that both sides need to be working from the same database, asking, “Does the database ESI have a concrete beginning or ending date or is it a “rolling” database where data’s added and deleted on a continuous basis?”

Database discovery is challenging and contentious, so know what you need and articulate why and how you need it. Be prepared to propose reasonable solutions that won’t unduly disrupt operations.

#### **18. Will paper documents be scanned, with what resolution, OCR and metadata?**

---

<sup>10</sup> Michael R Arkfeld, *Arkfeld on Electronic Discovery and Evidence* (2nd Ed. 2007); <http://www.lexisnexis.com/arkfeld/>



Paper is still with us and ideally joins the deluge of ESI in ways that make it electronically searchable. Though parties are not obliged to convert paper to electronic forms, they commonly do so by scanning, coding and use of Optical Character Recognition (OCR). You'll want to insure that paper documents are scanned so as to be legible and suited to OCR and are accompanied by information about their source (custodian, location, container, etc.).

### **19. Are there privilege issues unique to ESI?**

Discussing privilege at meet and confer entails more than just agreeing to return items that slip through the net. It's important to surface practices that overreach. If the other side uses keywords to sidetrack potentially privileged ESI, are search terms absurdly overbroad? Simply because a document has the word "law" or "legal" in it or was copied to someone in the legal department doesn't justify its languishing in privilege purgatory. When automated mechanisms replace professional judgment concerning the privileged character of ESI, those mechanisms must be closely scrutinized and challenged when flawed. Asserting privilege is a *privilege* that should be narrowly construed to protect either genuinely confidential communications exchanged for the purpose of seeking or receiving legal counsel or the thinking and strategy of counsel. Moreover, even documents with privileged content may contain non-privileged material that should be parsed and produced. All the messages in a long thread aren't necessarily privileged because a lawyer got copied on the last one.<sup>11</sup>

### **20. What search techniques will be used to identify responsive or privileged ESI?**

Transparency of process is vitally important with respect to the mechanisms of automated search and filtering employed to identify or exclude information, yet opponents may resist sharing these details, characterizing it as work product. The terms and techniques facilitating an attorney's assessment of a case are protected, but search and filtering mechanisms that effectively eliminate the exercise of attorney judgment by excluding data as irrelevant should be disclosed so that they may be tested and, if flawed, challenged. Likewise, if the defendant uses mechanized search to segregate data as privileged, plaintiffs should be made privy to same in case it is inappropriately exclusive, though here, redaction may be appropriate to shield searches tending to reveal privileged information.

### **21. If keyword searching is contemplated, can the parties agree on keywords?**

If you've been to Las Vegas, you know Keno, that game where you pick the numbers, and if enough of your picks light up on the board, you win. Keyword searching ESI is like that. The other side has you pick keywords and then goes off somewhere to run them. Later, they tell you they looked through the matches and, sorry, you didn't win. As a consolation prize, you may get the home game: a million jumbled images of non-searchable nonsense.

Perhaps because it performs so well in the regimented setting of online legal research, lawyers and judges invest too much confidence in keyword search. It's a seductively simple proposition: pick the words most likely to uniquely appear in responsive documents and then review for relevance and

*Never allow opposing counsel to position keyword search as a single shot in the dark. You must be afforded the opportunity to use information gleaned from the first or subsequent efforts to narrow and target succeeding searches.*

<sup>11</sup> See, e.g., *Muro v. Target Corporation*, 243 F.R.D. 301 (N.D. Ill. June 7, 2007) and *In re Vioxx Products Liability Litigation*, 501 F. Supp. 789 (E.D. La. Sept. 4, 2007)

privilege just those documents containing the key words. But according to Jason Baron, Director of Litigation at the National Archives and Records Administration, "Lawyers are waking up to the fact that keyword searching is subject to profound limitations in terms of accuracy and results."<sup>12</sup> Thanks to, e.g., misspellings, acronyms, synonyms, IM-speak, noise words, OCR errors and the peculiar "insider" lingo of colleagues, companies and industries, keyword search performs far below most lawyers' expectations, finding perhaps 20% of responsive material on first pass.<sup>13</sup>

Under the rubric of "concept search," technologies employing Google-like analysis are improving both the precision and recall of electronic search, but Baron cautions, "Despite the hype, artificial intelligence, data mining, and content analytics is just not sufficiently advanced to ensure that substantially all relevant documents in a large collection of ESI will be found."<sup>14</sup> Warts and all, keyword search remains the most common method employed to tackle large volumes of ESI, and a method still enjoying considerable favor with courts.

Baron notes that "keyword searches--indeed, any form of searching--is more effective when employed in an iterative way, as part of a cooperative and informed process."<sup>15</sup> In other words, never allow your opponent to position keyword search as a single shot in the dark. You must be afforded the opportunity to use information gleaned from the first or subsequent effort to narrow and target succeeding searches. The earliest searches are best used to acquaint both sides with the argot of the case. What shorthand references and acronyms did they use? Were products searched by their trade or technical names?"

Collaborating on search terms is optimum, but a requesting party must be wary of an opponent who, despite enjoying superior access to and understanding of its own business data, abdicates its obligation to identify responsive information. Beware of an invitation to "give us your search terms" if the plan is to review only documents "hit" by your terms and ignore the rest.

## **22. How will de-duplication be handled, and will data be re-populated for production?**

---

<sup>12</sup> Mr. Baron should know, as he is Editor in Chief of The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery (2007) and also responsible for searching through 20 million White House presidential emails in response to massive discovery in the *U.S. v. Philip Morris* tobacco litigation.

<sup>13</sup> See, e.g., The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery (2007) (describing the famous Blair and Maron study, which demonstrated the significant gap between the assumptions of lawyers that they would find 75% of the total universe of relevant documents, versus the reality that they had in fact found only 20% of the total relevant documents in a 40,000 document collection).

<sup>14</sup> Influential Magistrate, Judge John Facciola, mentions concept search in his opinion in *Disability Rights Council of Greater Washington, et. al, v Washington Metropolitan Transit Authority, et. al.* 2007 U.S. Dist. Lexis 39605, citing, George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 Rich. J.L. & Tech. 10 (2007).

<sup>15</sup> See, e.g., Paul, George L. and Jason R. Baron, "Information Inflation: Can The Legal System Cope?," 13 Richmond Journal of Law and Technology (2006), <http://law.richmond.edu/jolt/v13i2/article11.pdf>. See also, The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production, Comment 11.a (The Sedona Conference@Working Group Series, 2007), available at [www.thosedonaconference.org](http://www.thosedonaconference.org).

ESI, especially e-mail, is characterized by enormous repetition. A message may appear in the mail boxes of thousands of custodians or be replicated dozens or hundreds of times through periodic back up. De-duplication is the process by which identical items are reduced to a single instance for purposes of review. De-duplication can be *vertical*, meaning the elimination of duplicates within a single custodian's collection, or *horizontal*, where identical items of multiple custodians are reduced to single instances. If production will be made on a custodial basis—and depending upon the review platform employed—it may be desirable to request re-population of content de-duplicated horizontally so each custodian's collection is complete.

### **23. What forms of production are offered or sought?**

Notably, the 2006 Federal Rules amendments gave requesting parties the right to designate the form or forms in which ESI is to be produced. A responding party may object to producing the designated form or forms, but if the parties don't subsequently agree and the court doesn't order the use of particular forms, the responding party must produce ESI as it is ordinarily maintained or in a form that is reasonably usable. Moreover, responding parties may not simply dump other forms on the requesting party, but must disclose the other forms before making production so as to afford the requesting party the opportunity to ask the court to compel production in the designated form or forms.<sup>16</sup>

Options for forms of production include native file format, quasi-native forms (e.g., a partial export of data from a database), imaged production (PDF or, more commonly, TIFF images accompanied by load files containing searchable text and metadata), hosted (online) production and even paper printouts for small collections. It is not necessary—and rarely advisable—to employ a single form of production for all items; instead, tailor the form to the data in a *hybrid* production. TIFF and load files may suffice for simple textual content like e-mail or word processed documents, but native forms are best for spreadsheets and essential for audio and video. Quasi-native forms are well-suited to e-mail and databases.

A requesting party uncertain of what he needs plays into the other side's hands. You must be able to articulate both *what you seek and the form in which you seek it*. The native forms of ESI dictate the optimum forms for its production, but rarely is there just one option. The alternatives entail trade offs, typically sacrificing utility of electronic information to make it function more like paper documents. Before asking for anything, know how you'll house, review and use it. That means "know your review platform."<sup>17</sup> That is, know the needs and capabilities of the applications or tools you'll employ to index, sort, search and access electronic evidence.

---

<sup>16</sup> Fed. R. Civ. P. 34(b)

<sup>17</sup> If a question about your review platform gives you that deer-in-headlights look, you're probably not ready for meet and confer. Even if you're determined to look at every page of every item they produce, you'll still need a system to view, search and manage electronic information. If you wait until the data start rolling in to pick your platform, you're likely to get ESI in forms you can't use, meaning you'll have to expend time and money to convert them. Knowing your intended platform allows you to designate proper load file formats and determine if you can handle native production.

Choosing the right review platform for your practice requires understanding your work flow, your people, the way you'll search ESI and the forms in which the ESI will be produced. A platform geared to review of ESI in native formats must be able to open the various types of data received without corrupting its content or metadata. ESI can be like Russian nesting dolls in that a compressed backup file (.BKF) may hold an encrypted Outlook e-mail container (.PST) that houses a message transmitting a compressed archive (.ZIP) attachment containing an Adobe

## **24. How will you handle redaction of privileged, irrelevant or confidential content?**

Defendants often seek to redact ESI in the way they once redacted paper documents: by blacking out text. To make that possible, ESI are converted to non-searchable TIFF images in a process that destroys electronic searchability. So after redaction, electronic searchability must be restored by using OCR to extract text from the TIFF image.

A TIFF-OCR redaction method works reasonably well for text documents, but it fails miserably applied to complex and dynamic documents like spreadsheets and databases. Unlike text, you can't spell check numbers, so the inevitable errors introduced by OCR make it impossible to have confidence in numeric content or reliably search the data. Moreover, converting a spreadsheet to a TIFF image strips away its essential functionality by jettisoning the underlying formulae that distinguishes a spreadsheet from a table.

For common productivity applications like Adobe Acrobat and Microsoft Office, it's now feasible and cost-effective to redact natively so as to preserve the integrity and searchability of evidence; consequently, where it's important to preserve the integrity and searchability of redacted documents, you should determine what redaction methods are contemplated and seek to agree upon methods best suited to the task.

## **25. Will load files accompany document images, and how will they be populated?**

Converting ESI to TIFF images strips the evidence of its electronic searchability and metadata. Accordingly, load files accompany TIFF image productions to hold searchable text and selected metadata. Load files are constructed of delimited text, meaning that values in each row of data follow a rigid sequence and are separated by characters like commas, tabs or quotation marks. Using load files entails negotiating their organization or agreeing to employ a structure geared to review software such as CT Summation or LexisNexis Concordance.

## **26. How will the parties approach file naming and Bates numbering?**

It's common for file names to change to facilitate unique identification when ESI is processed for review and production. Assigned names may reflect, e.g., unique values derived from a data fingerprinting process called hashing or contain sequential control numbers tied to a project management database. Native productions don't lend themselves to conventional paged formats, so aren't suited to Bates numbering.

## **27. What ESI will be claimed as not reasonably accessible, and on what bases?**

---

portable document (.PDF). Clearly, a review platform needs to be able to access the textual content of compressed and proprietary formats and drill down or "recurse" through all the nested levels.

There are many review platforms on the market, including the familiar Concordance and Summation applications, Internet-accessible hosted review environments and proprietary platforms marketed by e-discovery service providers touting more bells and whistles than a Mardi Gras parade.

Review platforms can be cost-prohibitive for some practitioners. If you don't currently have one in-house, your case may warrant hiring a vendor offering a hosted platform suited to the ESI. When tight budgets make even that infeasible, employ whatever productivity tools you can cobble together on a shoestring. You may have to forego the richer content of native production in favor of paper-like forms such as Tagged Image File Format (TIFF) images because you can view them in a web browser.

Pursuant to Rule 26(b)(2)(B) of the Federal Rules of Civil Procedure, a litigant must show good cause to discover ESI that is “not reasonably accessible,” but the burden of proving a claim of inaccessibility lies with the party resisting discovery. So it’s important that your opponent identify the ESI it claims is not reasonably accessible and furnish sufficient information about that claim to enable you to gauge its merit.

Michael Arkfeld warns that, “Some defense attorneys take the position that additional burden or cost associated with any ESI makes it ‘not reasonably accessible’ and the requesting party must pay for its production.” Arkfeld agrees that’s a misinterpretation, but one that can prevail when parties or the court don’t make the effort to understand the amended rule.

The meet and confer is an opportune time to resolve inaccessibility claims without court intervention—to work out sampling protocols, cost sharing and filtering strategies—or when agreements can’t be reached, at least secure commitments that the disputed data will be preserved long enough to permit the court to resolve issues.

*The meet-and-confer session is an opportune time to resolve inaccessibility claims without court intervention--to secure a commitment that the information at issue will be preserved.*

## **28. Can costs be minimized by shared providers, neutral experts or special masters?**

Significant savings may flow from sharing costs of e-discovery service providers and online repositories, or by eliminating dueling experts in favor of a single neutral expert for thorny e-discovery issues or computer forensics. Additionally, referral of issues to a well-qualified ESI Special Master can afford the parties speedier resolution and more deliberate assessment of technical issues than a busy docket allows.

## **Endgame: Transparency of Process and Collaboration**

Courts and commentators uniformly cite the necessity for transparency and collaboration in electronic discovery, but old habits die hard. Too many treat meet and confer as a perfunctory exercise, reluctant to offer a peek behind the curtain. Some are paying dearly for their intransigence, sanctioned for obstructive conduct or condemned to spend obscene sums chasing data that might never have been sought had there been communication and candor.<sup>18</sup> Others are paying attention and have begun to understand that candor and cooperation in e-discovery isn’t a sign of weakness, but a hallmark of professionalism.

*Candor and cooperation in e-discovery isn’t a sign of weakness, but a hallmark of professionalism*

The outsize cost and complexity of e-discovery will diminish as electronic records management improves and ESI procedures become standardized, but the meet and confer process is likely to endure and grow within federal and state procedure. Accordingly, learning to navigate meet and

---

<sup>18</sup> Courts have sanctioned ESI discovery abuse for actions characterized as intentional deception: *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008); gross negligence: *Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 WL 2135798 (S.D.N.Y. Aug. 1, 2006); “reckless disregard:” *United Med. Supply Co., Inc. v. United States*, 77 Fed. Cl. 257 (2007); “purposeful sluggishness:” *In re Seroquel Prods. Liab. Litig.*, 2007 WL 2412946 (M.D. Fla. Aug. 21, 2007); “foot dragging:” *Toussie v. County of Suffolk*, 2007 WL 4565160 (E.D.N.Y. Dec. 21, 2007) and negligence: *Finley v. Hartford Life and Acc. Ins. Co.*, 2008 WL 509084 (N.D. Cal. Feb. 22, 2008). Increasingly, courts regard the duty to preserve and produce ESI as one mutually shared by client and counsel, and refuse to accept ignorance on either’s part as an excuse. See, e.g., *Qualcomm Inc. and Phoenix Four, Inc.*

confer—to consistently ask the right questions and be ready with the right answers—is an essential advocacy skill.