



ESI Collections: Reducing Costs, Minimizing Risk

Best Practices for eDiscovery Collections

by Chris Mashburn,

Director, Technical Consulting, Electronic Discovery, Inc.

January 2008

Executive Summary

After two decades of helping companies and law firms successfully manage eDiscovery projects, we've seen firsthand the essential value our clients derive from an upfront, focused and strategically thoughtful approach to the collections process. Time and time again companies have come to us with problems that could have been easily avoided by a more detailed, consistent and auditable collections plan with each action and decision being informed by and flowing naturally to the next logical step.

This white paper will address the importance of employing a sound collections process for electronic stored information (ESI) and offer guidance for creating your own defensible approach to collecting evidence. The following topics regarding eDiscovery collections will be covered:

- Balancing due diligence vs. full diligence
- Elements of Strategic ESI data preservation
- Collecting ESI data with production in mind
- How to get started without adding risk
- Deputizing the right person
- Keeping key custodian lists appropriately focused
- Avoiding unnecessary burden by mapping the matter, not the world
- The advantage of casting your ESI net just wide enough
- Documenting chain of custody
- Thoughtful approach to ESI backups and legacy media
- Knowing your collections service provider

No matter what you do or how carefully you do it, opposing counsel will, at the very least, want to know how you addressed the collections phase with an eye toward exploiting any perceived weakness in your approach or process. Being able to demonstrate on-going due diligence and reasonableness of approach to the court is critical. Even if the court does find some fault with your approach and asks for correction, if you've consistently employed sound guiding principles and can explain your approach, you won't find yourself in hot water.

Assessing and applying these guiding principles and chronological approach to the specifics of a given matter will allow you to move ahead with confidence that you've covered your bases and positioned your client well in the coming fray.

Due Diligence vs. Full Diligence

When it comes to collections, due diligence is absolutely critical, and may be even more so when the merits of a complaint aren't strong. Where many people go wrong is equating "due" diligence with "full" diligence. Effective, defensible collection is not just about being thorough, it is about being thoughtful. It's about taking the action that is most reasonable given the current information. To build a defensible collection strategy:

- Think through the collections process on the front end, and continuously relate it to the specific matter at hand.
- Cast your net just wide enough to catch all the fish you need, plus just a few more, for your specific case. Find the right balance between collecting too much and not enough.
- Know why you are doing everything you're doing; do it as consistently as you possibly can, and document it along the way.
- Demonstrate on-going diligence, good-faith and responsibility. For example, don't make the mistake of notifying custodians they're being relied on to preserve certain information and not require they acknowledge, understand and agree to follow the preservation directions. Likewise, for any ongoing preservation relying on individual custodian's continued assistance, a non-burdensome random sampling to ensure ongoing compliance with the preservation instructions should be defined and carried out on a regular schedule.

Create a strategy for ESI data preservation now

In light of new Federal Rules of Civil Procedure (FRCP), most corporate counsel now realize that you have to start thinking about collections strategy before the company faces litigation. A critical component in any proactive collection strategy is creating a formal, deliberate plan for what your Information Technology department will do. In absence of such a plan, more often than not corporate IT departments will keep everything to eliminate the risk of being asked later for something they no longer have. While this may seem the safest approach, it greatly increases your collection costs and legal exposure. Focusing on the benefits of decreasing a preserved data set via concept searching, search terms, date constraints, etc to afford attorneys a more focused, cost and time effective review of potentially responsive records is certainly useful. Often, this is represented visually as a funnel, with the preserved source data flowing into the top and, by way of the various culling processes, a significantly smaller, and more matter relevant review set exiting the bottom. **What's often overlooked is the opportunity to greatly narrow the amount of source data flowing into the funnel to begin with.**

You may not yet have an electronic discovery strategy in your organization. Increasingly, corporate legal departments are responsible for this function. This is an area where eDiscovery consultants like EED can add real value, offering practical guidance based on

their long history of assisting key stakeholders on the client side in mapping existing data topology, taxonomy and life cycle and enabling strategic consensus to the satisfaction of records managers, business unit leaders, corporate IT departments and legal counsel. The subsequent implementation of company mandated policies and clearly defined practices and protocols ensures a data lifecycle that retains what makes sense or is required for regulatory and legal hold compliance, disaster recovery and business continuity purposes as well as preserving the institutional knowledge that represents a defined strategic value for the company to maintain. Everything else, which doesn't provide recognized benefit but in fact constitutes a direct operational and potential legal cost liability, can then be legitimately excluded from ever being available to enter the top of the funnel diagram referenced above.

Slow down, planning is getting started

What many companies forget in their anxiety to show the court they've hit the ground running is that **gathering information and planning strategy show due diligence**. The alternative (moving ahead with collections before there's a clear plan) will certainly cost you. As you've probably gathered by now, collections involves a lot more than directing IT to go out and grab backup tapes for a specific period of time. Sound collections require forethought and strategy. Start with a collection planning session, and follow this chronology to reduce scope and burden:

- Understand the specific matter.
- Define criteria for identifying custodians and create your list.
- Define key data types.
- Define your timeframe constraints.
- Cast your net around just that data that applies to the matter at hand — plus slightly more.

The goal is to focus on the critical information, and review it as effectively and efficiently as possible. Remember to balance your collection with the organization's potential risk. For example, if your company stands to lose \$10,000 in the complaint, and your collection plan will cost twice that, something needs to be adjusted. A suit with an exposure greater than \$5 million is obviously a different story.

Also, while you absolutely want to document your final plan, keep in mind that any written (email) deliberations that occur while developing the plan may garner broader readership than originally intended. You might want to consider restricting these preliminary fact gathering and brainstorming sessions to discussions and work in progress private notes while establishing the details.

Deputizing the right person

If your house were on fire, would you ask the neighbor to put it out just because he or she was standing in your yard? Since your neighbor lacks the proper equipment, training and track record of successfully extinguishing burning houses, relying on their assistance creates an unacceptable risk of failure.

Companies often assume that because IT is already responsible for backups, it's logical and reasonable to make them responsible for preserving and collecting data when faced with a lawsuit. Unless IT has past experience and training with collections processes specifically tailored to the unique demands of at-need legal situations, nothing could be further from the truth. While IT may be technically capable and even willing, collection is about much more than technology. Methodology and process are critical, and you must have an audit trail and documentation to back you up in case you are questioned or challenged in court. Placing a person or group with no previous experience, training and historical track record of success in charge of collections to fulfill the exacting requirements of a legal matter may be risking charges of spoliation and lack of due diligence. Another consideration is that the person responsible for collections may be called before the court to explain exactly what, how, and why he/she did... You need to think about how well the person you assign this responsibility will represent you and your interests under the pressure of deposition.

The key point here is to designate an appropriate person for collections and get them the training they need before your company faces a lawsuit. For cases with significant exposure, seeking outside expertise for collections is critical.

Custodians: keep your list narrow, collect ESI data once

Just as you can increase costs and risks by preserving too much data, creating a custodian list that is too broad can have the same result. You may unintentionally expand the scope of the matter by automatically including, for example, all your executives, irrespective of their relationship to the specific case.

- To avoid over-inclusion on the custodian list, carefully define inclusion and exclusion criteria (based on the specific complaint) before you make your custodian list. Be thoughtful as well as thorough. As always, document your decision process so you will be able to articulate it to the court later.
- Within your list, you will find that some custodians are more critical than others some will be directly related to the case, while others only tangentially. It is typically justifiable (and defensible) to collect with these differences. For example, if based on the custodian's degree of relationship to the case, the burden of collection is too great to justify your costs, err on the side of slight over inclusion (more on this in Cast Your Net Just Wide Enough).
- Don't begin to collect until you feel reasonably confident about your list — collecting more than once, at different points in time, can lead to inconsistent results that may open you up to charges of lack of due diligence and even spoliation. In addition, before you collect you may want to plan for IT and legal to spend some time gaining an understanding of how custodians go about copying and migrating important data to folders designated for litigation. Without understanding how individual custodians are handling their data, creating a blanket protocol for everyone to follow may be risky.

- One last word regarding custodians: Only the attorneys should conduct custodian interviews, and these should be fully standardized and documented. As with every aspect of the collections process (we cannot emphasize this point enough), consistency in your process is critical to defensibility.

Map the matter, not the world

A common mistake in approaching collections is the failure to narrow the focus of the collection to the matter at hand. There is no need to analyze and understand, for example, a 10-year history of corporate infrastructure, migrations, upgrades, backup policies, etc. In most cases this is no more than a painful exercise. Much of the EIS (electronic stored information) you evaluate will be housed on backup tapes or similar storage — an area owned by IT. Putting IT on the spot can not only create confusion and even dissension in exchange for negligible results. You'll likely end up with a huge cache of information that's of little value to your collection process. So where do you start? Once you have an understanding of the specific complaint, you will next

- Identify your criteria for creating a custodian list.
- Create your list.
- Notify those custodians of the requirement to preserve data.

When you have narrowed your focus to the data you need, you can provide IT very specific parameters for data collection.

Cast your net just wide enough

When deciding how much to collect, err just slightly over and above what you believe is justifiable and defensible for the matter at hand. By limiting collections to what you know you need, you dramatically reduce your costs and risks. By going just a little broader, you help insure yourself against claims from the other side that you collected too narrowly. Remember due diligence is all about balance, and whether your approach appears reasonable and consistent to the court.

As an example, assume you have a list of key custodians and a list of secondary custodians. You have appropriately distinguished between them in your approach by limiting collections for the secondary group. However, you discover along the way that one of your key custodians has exchanged a great deal of email with one of your secondary custodians. You make the decision to collect for that specific secondary as if they were a key custodian.

Documenting chain of custody

Before you get started, a word or two about the chain of custody. You must document that any physical evidence has remained within your control at all times to demonstrate that the integrity of your data has not been compromised. This documentation is important, but there is no need to go to extremes. For example, FedEx and UPS are generally considered reliable and reasonable by the court. There is usually no need to task an employee with driving cross-country to hand deliver documents to an office on the opposite coast.

Collect ESI data with production in mind

It's important to have the end game in view from the very onset of data collection. Look at production specifications prior to collection. If meet and confer sessions haven't achieved agreement on this prior to needing to collect, then it makes sense to collect in a manner that keeps all options available. For example, the date and time when someone received a Word document may be critical. If metadata was not preserved during the collections process (e.g., if files were copied/pasted from a file share), that original information may be lost or overwritten.

Be thoughtful in your approach to backups and legacy media

Backups are of obvious importance to the collections process. Very little litigation involves only what currently exists on servers or desktops. If you have thoughtfully preserved your data by preserving only enough to cover records management, disaster recovery, and historical requirements, your job is going to be that much easier. The next step is to look at differences between backups, and though it may seem counterintuitive, start with the long timeframes and move to the short — that is, first compare years and quarters, then months, weeks, and so on as appropriate. This approach will give you a much better idea of how much data you need to sift through.

If your backups are outsourced, take extra care. Don't rely on a third party to take data preservation as seriously as you do. If you have outsourced archiving, it is critically important that you confirm they are abiding by your preservation order and that you have a full understanding of how they have been handling your data. The court will not excuse you for negligence on the part of a vendor.

And finally a note about legacy media: archeology is a dirty business. Legacy media can introduce a whole host of challenges of its own, including missing or inconsistent labeling, incomplete or damaged data, and outdated technology. FRCP rules allow some wiggle room when it comes to accessibility — if you can get even close to the same information from a more accessible source, you may be justified in excluding legacy media.

Know thy collections service provider

For many companies, working with a consultant can bring peace of mind and dramatic savings. eDiscovery companies like EED allow you to leverage their years of expertise in defensible collections process and discovery strategy, ensuring your requirements are met and your interests are protected. Here are a few parting cautions when engaging with consultants:

- The buck stops with you. Your consultant must have a track record of defensible collections, and they must clearly explain and justify their approach. You make the call. If something is amiss in your process, no judge will accept "our consultants made us do it."

- Know what you are doing and why. Consultants can and should tell you what has been done in similar cases, share solid guiding principles, employ technology to reduce your costs, and help you ensure your process is auditable. However, it is the attorney who will have to stand before the judge and justify the approach.
- Do not rely too heavily on technology. The right technology can reduce both your timeline and your costs, but the hottest new technology won't fix a broken process. Technology must be coupled with proven, defensible methodology, which only the most experienced consultants can offer.

Conclusion

A white paper on collections could run into hundreds of pages. We have tried to hit the highlights — some of the most common issues we've encountered in two decades of advising clients on collections and managing large collections projects.

Let's recap some key points..

- Reasonableness of approach will get you far with the court. Be thoughtful as well as thorough. You cannot and should not preserve or collect all data. Target due diligence rather than full diligence. It really is a win-win situation: you'll create a collections plan that minimizes both your costs and risks.
- Focus on the matter at hand. Relate every single thing you do back to the matter at hand. This approach will help you keep your focus and narrow your scope to only the critical information. When you have a good idea what that information is, widen your net just a little so you can demonstrate to the court you went above and beyond.
- Variance is the enemy of defensibility. Documentation and audibility is critical, but we can't overstate the value of consistency. The best way to show the court that you believed you were doing the right thing, and that you believed your process was appropriate, is by following it consistently.



Electronic Evidence Discovery, Inc. (EED)

EED is the pioneer of litigation hosting technology and electronic discovery services. For more than a decade, EED has reduced the cost and time required for eDiscovery in thousands of high risk cases. Our eDiscovery experts, who come from law firms, corporations, and the technology industry, understand the complexity and risk involved in evidence management for large matters. Our clients — 60% of the Fortune 500 and 45% of the NLJ 250 — value our unmatched expertise, thoughtful leadership and results. Through integration of our proven methodology, people and tools, EED delivers results that meet and surpass our clients' expectations. EED is headquartered in Kirkland, WA.



Electronic Evidence Discovery, Inc.
Worldwide Headquarters
Plaza at Yarrow Bay

3933 Lake Washington Blvd. NE
Suite 200
Kirkland, WA 98033

Tel: 206.343.0131
Fax: 206.343.0172
Email: info@eedinc.com