



100 California Street, Suite P-10, San Francisco, CA 94111 | 415.392.2900 | www.sanfranciscolegal.com

Eight Tips for Improving the Data Collection Process

1. There are significant risks to a flawed process ... so get one in place EARLY

There's significant risk in not having a process in place for effective data preservation and collection. For example, if a litigation hold process isn't started quickly after a complaint is filed, it's very possible that a client will fail in their duty to preserve data. In addition, if data isn't collected in a forensically defensible manner, or if critical data is ignored, law firms and corporations can be exposed. The financial and legal risks of such process failures are well documented in many judgments that have come down in recent years, such as the one against Morgan Stanley. The critical takeaway is: Put an effective process in place as early as possible once a matter is live.

2. Identify, then preserve, then collect

An effective process starts with *identification* – figuring out what data you have on your hands. A network diagram and a data inventory need to be created. Once that's done, then preservation becomes much easier. The next step is to make sure the data is *preserved*. The duty to preserve begins at "reasonable anticipation" of litigation. A litigation hold notice must go out in a timely manner and be clearly communicated to all relevant parties so that the right data is preserved, and it's preserved in its original form. Then the *collection* can be planned and executed. The data ultimately collected can be, and generally is, much more targeted than the data preserved. The ERDM is an excellent template to follow (www.edrm.net). It lays out the stages for collection very clearly.

3. Early communication between attorneys and technical teams saves money

Multiple players impact an effective collection strategy, and they need to be talking to each other. Clearly, inside and outside counsel know the most about the core tenets of the case. Increasingly, law firms and corporations also have designated e-discovery counsel specialists. Then there are the IT and litigation support teams at the client and/or law firm, often supplemented by a vendor partner, who can give the primary technical input to define a legally defensible and cost-effective process. What's important is that the parties start talking to each other early. When these groups meet and talk early on, the process has a good chance of running smoothly and being more cost effective. The tough part is typically convincing the attorneys to spend time on the technical issues up front. So often, if that doesn't happen, the review team ends up reviewing large amounts of irrelevant information.

4. Each situation is unique – design the right collection plan, not a one-size-fits-all

There are different solutions for different cases. It's imperative that the technical team – whether from the law firm, a vendor, the client, or a combination – spend time with the attorney team to understand what the matter is about before they start on the collection. It's critical to ask, "What is at issue here, what are the allegations," and then design collection around it. A securities fraud matter may be very email intensive, a patent case may focus primarily on PowerPoints or engineering documents, and a sexual harassment or theft of trade secrets case might rely heavily on data hidden in the unallocated space (for example, deleted documents or email sent from yahoo or gmail accounts).

5. Try to collect less, not more – and leverage an effective post-collection filtering process to keep review costs down

Data volumes continue to grow at an explosive rate, resulting in ever increasing review costs. The review process is still by far the largest component of the overall cost of litigation. As a result, there's a huge return on efforts made to reduce the amount of data ultimately reviewed. A targeted data collection strategy, combined with effective data filtering prior to review, is critical. For example, start with key custodians first. Think about using targeted data collection options to gather only specific file types and/or date ranges. Spend time with the individuals you're collecting from to really understand what information they have and where it's stored. And look at filtering options post collection, which include key term searches, as well as more advanced tools such as email domain filtering, concept clustering, email thread analysis, and so on.

6. Whoever does the collection, make sure it is defensible and documented

There are situations in which clients do collections, where outside vendors do them, and in some cases even where law firms do them. Often clients aren't set up to handle collections defensibly, and don't want to take on the responsibility of documenting the process, and, if necessary, having to testify to it. In other cases, clients have very sophisticated collection tools and teams. What's important is that whichever route is chosen the process must be clearly documented and legally defensible tools must be used to collect the data.

7. Stand by the three primary tenets of the Amended FRCP

There's much detail in the Amendments to the FRCP, but there are three primary tenets:

1. Give early attention to e-discovery
2. Meet and confer on the issues
3. Be transparent

Even if a mistake is made, if these three tenets are followed, many legal and financial risks will be avoided. Dumping, while tempting, typically doesn't work and instead creates more headaches and cost for both sides. It's far better to hold constructive meet-and-confer sessions with the other side and deliver more targeted data. Transparency is also becoming more and more critical. Document everything and be open. Even though the amended rules have been in effect 18 months, only now in the past few months are we really starting to see detailed initial disclosures where everything is laid out (for example, a full description of the data network/system being shared). Once all of the information is out there, the two sides can make decisions – e.g., ignoring cell phones and voicemail in the collection. Transparency can also be valuable with proprietary data formats. If there's a proprietary data format, it's advisable to work out a way of being transparent and providing the other side access. The same logic should be applied to back-up tapes. Be transparent about what you have and your process. And with more disclosures, judges can be more effective in deciding on discovery issues.

8. Education, education, education

There's a significant education process that still needs to happen around the data collection process, and more broadly about e-discovery. This is a rapidly evolving area. Attorneys and clients who don't get educated run major legal and financial risks. In particular, attorneys and corporate clients need to:

1. Educate themselves on the fundamental process of effective data collection
2. Learn who's available to help – from other experts within their firm, to experts at the client, to vendor partners – and when to talk with them
3. Understand that this isn't an event, it's a process – it will be a repeated game

These tips were compiled by Christian Lawrence, CEO of San Francisco Legal, based on discussions at a BALSP panel that San Francisco Legal sponsored in July at Heller Ehrman. The panel featured Helen Marsh, e-Discovery counsel at Kecker & Van Nest and Ben Suess, litigation support manager at Heller Ehrman

© 2008 San Francisco Legal.