Do Your Clients Have Litigation Preparedness Plans?

By Larry G. Johnson, J. D.

It is a rare corporation that does not have in place a detailed and reliable Disaster Recovery Plan. In the event of a fire, flood or hurricane, IT staffs around the world are able to restore networks with minimal data loss and downtime, thanks to carefully devised and implemented backup and off-site data storage procedures.

And remember Y2K? Many a company dodged a bullet by upgrading their computer systems in advance of January 1, 2000, saving themselves from potentially very costly data foul-ups and service interruptions.

But how many companies have a Litigation Preparedness Plan? In terms of costs and disruption, the "disaster" of being sued and subject to the realities of electronic discovery requirements could dwarf the costs of Y2K or an earthquake. The solution, of course, is to insure your client has a plan in place that anticipates litigation and reduces substantially the e-discovery target.

Attendees at our national continuing legal education presentations and our law firm and corporate counsel clients are in almost uniform agreement that digital data risk management is a good idea, but since it's not a priority, it can be put off indefinitely. Apparently there are a lot of optimists out there who conclude, "There's no need to worry since nobody's suing us and we have a good track record."

The reality, of course, is that there are many things to worry about: will your client, once sued, be able to avoid the hazards of inadvertent spoliation due to mismanagement or lack of management of its digital data? Does it have so much old or useless computer data stored in so many places, known and unknown, that it may never respond in time to discovery requests or meet court-ordered deadlines? Will it be forced to forego good defenses or counterclaims because nobody knows for certain where the documentary proof is to support them?

Good for Your Client, Good for You

Setting up and enforcing an electronic records retention policy is one kind of preventive legal medicine that, if properly administered, can substantially reduce the risks of money sanctions or worse for failing to respond timely to discovery. Your clients should think of it as a kind of insurance.

From the perspective of your own law firm's growth, think of how many clients you have who are currently *not* being sued compared to those who are. You have an opportunity, through teaming with a technical consultant, to provide a valuable proactive service for your client while at the same time creating a new profit center for your firm.

Step One: Getting Your Client to "Know What It Knows"

We at Legal Technology Group, Inc. are often involved in cases involving Fortune 500 companies where their electronic documents (e-mails, spreadsheets, word-processed documents, databases, CAD files, PowerPoints, etc.) are typically stored on many different servers at multiple locations, often throughout the world, and feature documents in more than one language. Many of the servers perform discrete enterprise functions that do not require them to integrate with other servers. An e-mail server in Pennsylvania, for example, does not need to interact with a database on another server in Florida handling customer purchase orders, invoices and delivery fulfillments. Yet once sued, a company's lawyers must be able to certify per Rule 26(g) that responses to electronic discovery requests are "complete and accurate as of the time made." That means all data sources need to be identified and reasonable queries made of the data, as well as of the people who created it, as part of a bona fide search for responsive documents, regardless of format. Any fraud or falsehoods in that regard can result in severe sanctions for both the lawyer and his or her client.

The first step is to prepare your client for the possibility that in the event of litigation, some or all of the information on some or all of its enterprise servers may have to be aggregated in one place. That could implicate some rather extensive electronic real estate. Your client's electronic data universe could consist of trillions of bytes (terabytes), the equivalent of millions of pages of paper documents. Worse, all of your client's backup tapes everywhere are also subject to the same "find and aggregate" requirements, even though the result is the accumulation of potentially hundreds of duplicates of the same document that have been backed up over and over again onto tapes or passed around to others in the enterprise where the documents land on numerous desktop hard drives.

And don't forget those dusty old WANG tapes that sit on a shelf in a warehouse somewhere, simply because nobody felt they could just be discarded. Although the equipment necessary to read those tapes may not exist and the personnel familiar with the files or how the software worked long gone, even those documents must be examined for relevance if nobody knows for sure what is on them. A specialty vendor may have to be hired to decipher what everyone suspects is just so much old junk.

Cull and Review

Once aggregated, all this data then has to be processed:

install and application software files eliminated, so only human-generated documents remain; duplicates removed but accounted for; password-protected files opened; compressed ("zipped") files extracted; viruses and destructive "trojan" programs quarantined; and corrupted, damaged or unreadable files isolated and accounted for. That's just the culling part.

After culling the data to a smaller review set comes the document review process. Doing it one page at a time in popular digital document review programs such as Concordance or Summation may not only require an army of associates and paralegals, but more time than is available. For example, it has been calculated that for one person to review 3 million documents (not unrealistic in today's digital data glut[1]), at a rate of 20 documents per hour in a 40-hour workweek, it would take 750 years to complete the job.[2]

But guess what? Not only do you not have 750 years, or 7.5 years if you put a 100 reviewers to work on the case full time, you quite likely don't even have 90 days if you are in federal court (or some state courts) because your client has to comply with the recently revised Rule 26(a)(1).[3] Your client's duty to disclose its case in chief, including all supporting documents, begins *at the start of the lawsuit*, and *without the other side having to request those documents through discovery*.

Here are some words to contemplate from Rule 26(a)(1) establishing the short fuses for compliance:

> These disclosures must be made at or *within 14 days after the Rule 26(f) conference* unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in the circumstances of the action and states the objection in the Rule 26(f) discovery plan. In ruling on the objection, the court must determine what disclosures—if any—are to be made, and set the time for disclosure. Any party first served or otherwise joined after the Rule 26(f) conference must make these disclosures *within 30 days after being served or joined* unless a different time is set by stipulation or court order. A party must make its initial disclosures based on the information then reasonably available to it and is not excused from making its disclosures because it has not fully completed its investigation of the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures (*emphasis added*).

You can hope for some relief through stipulation with the opposing side or by the court's discretionary powers, but don't count on it if your opponent or the judge plays hardball. Note, too, that there may be room for maneuver in the words "disclosures based on the information then reasonably available to it," but *unavailability* of e-documents based on the chaotic state of a corporation's electronic data due to lack of managing that data may not evoke much sympathy from the judge.

Stemming the Tsunami Waves of Digital Data

An Electronic Document Retention Policy is an important pillar for the Litigation Preparedness Plan ("LPP"). The LPP can then not only build on the reduced document population that results from the retention policy, but can also benefit greatly from technologies that intelligently group documents by content so that they can be classified by users dynamically as needed, and among which newly created documents can be integrated. In gross terms, this is where knowledge management (beneficial beyond the requirements of discovery) meets effective litigation support. And content-analysis software makes this part of the LPP easier to implement than most lawyers or even professional records managers appear to appreciate.

The LPP, by the way, does not have to be perfect. Its primary functions are to provide a reliable mechanism to avoid spoliation and to offer an acceptable level of probability that irrelevant documents can be identified and ignored. (Removing haystacks can be as important as finding needles in relevant haystacks!) Then, pursuant to Rules 26(f) and 16(b), court and counsel can develop additional ways to reduce the burdens of the initial disclosure under Rule 26(a) and subsequent e-discovery requests, including the following strategies, established either by agreement or through court order:

1. Sampling a small subset of the likely sources of potentially relevant information first, then deciding from the results where and when to seek further discovery based on what is revealed in the sample. See, e.g., *McPeek v. Ashcroft* 212 FRD 33 (DDC 2003) (sample of one e-mail box for e-mails over a period of one year before allowing broader e-discovery and deciding who pays for it).
2. Setting date ranges for document processing and text searches.
3. Limiting initial e-mail production to the mailboxes of key witnesses.
4. Appointing a neutral officer-of-the-court third party expert as the collector and repository for all parties' electronic data, assuring uniformity of processes and deliverables. See, e.g., *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999).

5. Selecting a Special Master, usually an attorney with expertise in e-discovery and digital data technologies, to rule on electronic discovery motions.

6. Imposing cost sharing that promotes production of readily available business documents but places on the requesting party the cost of anything "extraordinary," such as reconstruction of deleted files or file fragments by computer forensics experts, using "balancing tests" like the one set out in Texas Civil Rule 194.6 or weighing the several criteria outlined by Judge Scheindlin in *Zubulake v.UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y., May 13, 2003).

7. Agreeing to e-data exchange protocols that promote cost-effective procedures and "rolling productions" of documents as they become available.

8. Agreeing to use data mining technology that reduces the inefficiencies and inaccuracies inherent in keyword text searches only, by utilizing software and procedures that group documents (even paragraphs within documents) according to thematic content.[4] Major vendors of emerging document "context searching" technologies include DolphinSearch, Attenex, Engenium, Fios and Syngence.

The Better Way: An Ounce of Prevention

A good fire department is one that not only puts out fires but prevents them in the first place. A properly designed and enforced e-data retention policy can accomplish at least three things that have great ancillary benefits to the efficient operation of a commercial enterprise:

1. Reduction of its digital data stores by a robust, routine deletion of all emails after a "short-fuse" period of 30, 60 or 90 days. Procedures can be put in place to tag and archive mission-critical or important historical e-mails, but all others are eliminated by a no-nonsense, kill-all policy.

2. Reduction of duplicate documents in backup tapes by using filters to generate non-redundant and partial backups of newly added data only.

3. Use of content-organizing data mining technologies *before* litigation to identify and isolate files that have no current value and eliminating them using objective criteria for whole document populations (as opposed to potentially suspect ad hoc criteria applied to individual documents; that approach can invalidate a document retention program and expose a party to spoliation sanctions).

Of course, the rules change significantly once your client is sued or a lawsuit can be reasonably anticipated. Any documents removed at that point open your client to potential spoliation claims and the severe sanctions that can ensue. So the only really good time to insure against e-discovery excess and litigation unpreparedness is for your clients to get things in order before any claims loom on the horizon.

Not only do legally and technically defensible electronic document risk management policies reduce expenses and inexcusable delays in any future litigation, they also bring together an enterprise's document universe in a way that makes true knowledge management possible. A company that "knows what it knows" is less likely to needlessly duplicate work already done by somebody else in the enterprise or lose precious ideas that come only once in a lifetime.

Endnotes

[1] See, e.g., *Rowe Entm't, Inc. v. William Morris Agency, Inc.,* 205 F.R.D. 421, 429 (S.D.N.Y. 2002) (electronic data is so voluminous because, unlike paper documents, the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it), aff'd, 2002 WL 975713 (S.D.N.Y. May 9, 2002).

[2] John C. Tredennick, Jr., "Moving From 'BC to AD,'" Law Practice Management, May/June, Vol 29, Issue 4.

[3] The old rule, revised in December, 2000, allowed district courts to opt out of the disclosure requirements. The change by the U.S. Supreme Court eliminates the option. For more about the implications of amended Rule 26(a), see my white paper, "New Amendments to Rule 26 Dictate Use of Electronic Discovery Technology" under "White Papers, Links" at www.legaltechnologygroup.com.

[4] Page-by-page human review of documents, though in the past quite profitable for law firms, is becoming, as mentioned previously, increasingly difficult to impossible. Text-matching searches are also being superceded in accuracy and completeness by semantic context search technologies, i.e. ranking and matching documents by their meaning.

Larry Johnson has been a Seattle trial lawyer since 1974. He is president of Legal Technology Group, Inc. (www.legaltechnologygroup.com), providing electronic discovery consulting, digital data expert witness services, risk management solutions and due diligence reviews of litigation support technologies for law firms and their clients.

Reprinted with permission from *Digital Discovery & e-Evidence*, Volume 3, Number 8, pages 8 - 10. Copyright 2003 by Pike and Fischer, Inc. For more information on *Digital Discovery & e-Evidence*, call 1-800-255-8131 ext 248.