Late Night With eDiscovery Nightmare-man? Top Ten Ways to Help Your CEO Sleep More Easily . . .

ROBERT D. BROWNSTONE

FENWICK & WEST LLP

Many an organization waits until it has seen the corporate body on the table in a lawsuit or in a government proceeding before implementing an electronic-discovery preparedness program. Often, nothing short of an expensive, stressful litigation kluge is sufficiently compelling.

Doom and gloom predictions of the staggering costs of litigants' collection, processing, review and exchange of terabytes of electronically stored information (ESI). Nor do war stories about night after night of waves of e-mails and electronic documents engulfing the electronic discovery (eDiscovery) process – and thus drowning a lawsuit before a judge or jury ever gets a chance to decide who, if anyone, wins the case.

So, without any guarantees other than "Do try this home," . . . and, with apologies to David Letterman, . . . from the home office in Silicon Valley . . . in chronological order along the litigation timeline . . . drum roll, please . . . here are The eDiscovery Guru's Top Ten Tips. . . .

10. Less is More, a/k/a Destroy or Drown

Day-to-day efficiencies and litigation preparedness can ensue when an organization develops and implements a "Records Retention" policy and program. As the U.S. Supreme Court ruled unanimously in 2005 in the *Arthur Andersen* case, a "retention" policy is actually a *destruction* policy, designed to keep information from getting into the hands of others, including the Government.

So routine disposition of old stale, unneeded and duplicative ESI is the first objective. Having less information and knowing what the company has – and where – should enable more effective operations. An added benefit is shrinkage of the data set subject to processing – and possibly to exposure to an adversary – in response to a future lawsuit, a non-party subpoena in someone else's lawsuit or a government inquiry.

9. Sing Kumbaya.

In developing the appropriate parameters of an effective, defensible retention/destruction program, make sure that folks from the Legal and IT Departments collaborate. If the key in-house lawyer or outside counsel is from Mars and the essential IT leader is from Venus, then use an interplanetary translator to help develop litigation-preparedness program. Then everyone can gets together and harmonize on the same tune.

8. Preserve or Perish.

Have a "litigation hold protocol" that assigns certain significant duties to one key person, usually a lawyer but sometimes a C-level executive. He or she will decide whether or not a legal dispute is "reasonably anticipated" such that a "litigation hold" must be issued to preserve all potentially discoverable information. In addition, he or she will oversee the implementation of the hold.

Without an adequate process *and* memorialization of steps taken – and steps not taken – a company can have a very hard time defending itself against a "spoliation" (illegal destruction) contention raised down the line by a litigation adversary. On the other hand, a routine, "real" and documented approach can insulate against risk. The elephant in the room is that a spoliation finding could morph into a dismissal or default judgment by a judge who becomes frustrated and suspicious.

7. Build the Three-Legged Stool.

Form an ESI/eDiscovery task force that will stand tall in three arenas: 1) knowledgeable people; 2) a powerful computer-technology platform; and 3) a set of up-to-date written protocols to guide the in-house and outside teams through the process. At a minimum, make sure you have in place a short list of trusted outsiders with expertise in collecting live data and forensically recoverable data.

6. Preserve, Protect, Defend.

Preserve as broadly as possible without hampering the IT Department' s operations and budget. As to the to-be-collected subset of the preserved ESI, make sure your techie has: sufficient skills to avoid altering metadata (creation date, last modified date); the wherewithal to maintain chain-of-custody information; and the wisdom to segregate a pristine data set so processors and reviewers are only turned loose on a working copy.

5. Natives Need Not Make You Restless

Consider exchanging email messages and electronic files (especially spreadsheets) in their original/"native" formats. Harness the technology know-how and an agreed-upon method of electronic-fingerprinting to prevent alteration. In many a case, "going native" can avoid huge out-of-pocket costs of converting

thousands of items to an image format (typically TIFF). Work with the other side up front to enter into a clear written agreement ("stipulation") as to the format(s) of exchange of ESI.

4. Get M.A.D.? Then Get Even.

Be careful what you request from the other side as that adversary will assuredly request the same from you. When two companies apply the Mutually Assured Destruction (M.A.D.) principle, they can take off the table costly volumes of data, such as digital voicemails and back-up data created prospectively. Then hopefully the eDiscovery playing field can be as even as possible.

3. Cooperate to Cull Aggressively and to Preserve Clawback Rights

The less ESI that gets reviewed by lawyers, the less the discovery costs will be. So, as much as possible before the review team launches in, cull down the data set by employing objective criteria, subjective criteria (search methodology) and concept-searching software. At an early stage, the lawyer most familiar with the substance of the case should spend some time surfing and searching the ESI. Then, based on his/her first cut, alter the review subsets and strategies accordingly.

Early in the case, see if you can cooperate with the other side to set respective expectations for culling efforts. At the outset, also use best efforts to reach agreement with the other side as to the mutual right to "claw-back" privileged information that, given high volumes of ESI, might get through inadvertently. Get the judge to sign on to the clawback agreement so your company will be protected in the current suit and future lawsuits into which the inadvertently produced ESI could wend its way.

2. QA/QC

Periodically use Quality-Assurance (QA) tests to make sure the review is not generating an over-inclusive or under-inclusive data set. Then, before the ESI goes out the door, use some Quality-Control (QC) testing before. When agreeing with the other side to a production deadline, build in a cushion for QA/QC on your end. In general, consider involving a search-methodology expert. You may need him or her later on if the other side challenges how you got from Point A (tons of collected ESI) to Point B (production of a much smaller subset). One key culling arena in which that expert might be valuable would be the segregation of ESI protected by attorney-client privilege.

1. Never Drop Your Laptop Bag and Run.

When urging his law students to never back down, the legendary, 50-plus-years Brooklyn Law School Professor Joseph Crea has always exhorted: "Never drop your briefcase and run!" In today's digital wild west of eDiscovery, a more modern mantra – for lawyers and non-lawyers alike – might be "Never drop your laptop bag and run!"

Some day all of us will be copacetic with ESI and the lawsuit discovery process will be coextensive with eDiscovery and. At that point, routinized court-endorsed people-plus-technology processes will enable all litigants to more readily get to the merits. Until that day arrives, dig in, learn as much as you can and start building repeatable, efficient approaches.

*** NOT LEGAL ADVICE.** *Robert D. Brownstone, Esq. is the Technology & eDiscovery Counsel and Electronic Information Management (EIM) Practice Group Co-Chair at Fenwick & West LLP, a Silicon-Valley headquartered law firm providing full-service to hundreds of prominent high-technology and life-sciences companies. Mr. Brownstone also teaches eDiscovery Law & Process at two San Francisco Bay Area law schools. His full biography, extensive bibliography and contact information are available at fenwick.com/attorneys/4.2.1.asp?aid=544.*

Originally published on Forbes.com