BAR BULLETIN

KCBA KING COUNTY BAR ASSOCIATION

Justice... Professionalism... Service... Since 1886

This is a reprint from the King County Bar Association Bar Bulletin

February 2016

Trust Yourself To Conduct Early Assessment of Electronic Evidence

By Larry G. Johnson

When it comes to early assessment of your client's case to determine whether settlement or summary judgment may be the best course of action, that task can rarely be accomplished without examining the available electronic evidence. Because just as bank robber Willie Sutton famously said when asked why he robbed banks — "because that's where the money is" — so in today's litigation world, electronically stored information ("ESI") is where most of the evidence is.

But like many lawyers you may think you don't have the technical competence or expertise to investigate computer-generated evidence on your own. So, you may delegate this vital task to a subordinate such as a paralegal or in-house IT person and hope for the best.

But when you do that you run several major risks, including these:

Neither an in-house IT person or "computer guru" paralegal will likely have the unique skills required for proper examination of digital evidence.

Every law firm seems to have a staff person who is considered the "go-to guy" for computer issues. I like to call that person "Jenny." She's the one you always ask to get you unstuck from some mess you made in an Excel spreadsheet or who knows how to find an old email in your Outlook mailbox. You think she can fix anything.

Or there is John, who manages your firm's computer network system. He also knows a lot about computers, but his job is chiefly to keep the electronic plumbing of your firm's network in working order. He or she most likely knows none of the many software tools e-discovery experts utilize to find relevant evidence.

Without the expertise related specifically to e-discovery, here are examples of some of the common mistakes a Jenny or John can make:

• Using the "find" function in Outlook to search emails limits you to single-word search terms and consequently produces far too many "false positives." More refined results come from the use of combinations of search words that occur in Boolean searches (e.g., "oranges AND apples") or proximity searches ("'John' within 3 words of 'Smith'"). Seemingly counterintuitive, the more complex the mix of search terms used in a search, the more focused and reduced is the resulting set of responsive documents containing "hits."

• The "find" feature used to search emails in Outlook does *not* search the email attachments. The most important documents in an enterprise are often shared with others via email attachments, and Outlook "find" searches will completely miss those.

• Loading and searching a custodian's emails in Outlook changes the metadata. Do you want to be called as a witness to testify about the spoliation of evidence?

• A further problem when limiting your search for responsive emails within custodians' Outlook mailboxes alone: Important emails may be overlooked that were saved or archived and reside outside the user's mailbox (e.g., in a separate folder, public folders, offline storage devices, and network or cloud archives) — places where the in-house guru would not likely go to search.

• Insisting on producing TIFFs or PDFs instead of native files (the federal rules and their commentary strongly imply that native file format is the preferred way to produce ESI).

• Defaulting to a "one-time, get-it-all-now" set of search terms and culling of all data, rather than intelligently starting with the most likely custodians with evidence first and using just a few key search terms in combination, then letting the results inform further searches in an iterative, probabilistic manner.

• Failing to "de-dupe" files and remove duplicates across all custodians' files as a whole (while also preserving the option to keep an audit trail of all duplicates if there is a critical document and an issue arises about who had it and when).

• Going through the document review death march of looking at one doc at a time, rather than viewing a chronological overview of lists of "hits" within the context of lines of text before and after the hits, so that one can scroll quickly through scores of worthless documents rather than doing endless zombie point-and-clicks to wade through documents one at a time.

• Ignoring date metadata that would exclude docs that fall outside an agreed relevant time frame. There is a way to automate that process to significantly reduce the population of documents to review.

• Failure to take advantage of cost savings and efficiencies in using Rule 26 to limit e-discovery scope and amount. Jenny and John will probably have no

clue about Rule 26 and its many potential uses.

• Missing key data that may reside uniquely on overlooked devices such as smartphones, voicemail, thumb drives, online social media, backup tapes, databases, SharePoint, etc.

Just as you don't have expertise in every field of the law, so it is with in-house computer geeks: Their expertise is equally compartmentalized and rarely attuned to e-discovery technologies. In addition, few IT people have the certification or training in computer forensics to recover intentionally or inadvertently deleted data.

Third-party vendors are motivated to maximize profits and overdo e-discovery unnecessarily.

Nor should you simply delegate early case assessment to an outside vendor. Too often, third-party e-discovery vendors process too many data sources and data types because that is how they make money, whereas an intelligent early case assessment by you, carefully managing a vendor, would prevent a lot of e-discovery overkill.

Further, even though vendors may claim they have tech-savvy lawyers on staff who understand the litigation workflow and what litigators need, that is very rarely true. I have yet to meet a vendor staff attorney who had ever tried a case and what it takes to prepare one.

So, bottom line: A simple, but not so readily obvious, fact is that the person who should be most engaged in first looks at the digital evidence is *you*, the lawyer. Managing e-discovery effectively requires understanding the very core things you learned in law school and put into practice every day, such as: What are the key issues in the case? Who are the key witnesses? How strong is the evidence to support the other side's case? What aspects of the law affect relevance (e.g., statute of limitations; privileged communications; parol evidence)?

In an early case assessment, you are the one best qualified to recognize "the good stuff" when you see it.

So, here are some tips to help you get a handle on the ESI at the 30,000-foot level when doing an early case assessment:

1. Do use a competent e-discovery lawyer or third-party vendor to assemble and cull the masses of ESI in such a way that you can readily get a workable overview of it.

This means managing the vendor by making sure you limit their efforts to:

a) the key witnesses you identify whose data you will examine;

b) using date and time stamp metadata embedded in every electronic document so you eventually look at only files within a given relevant date range;

c) cull files by file type (e.g., do photos and videos really matter for your case?);

d) eliminate duplicate files (e.g., files that have the same digital fingerprint known as a "hash value");

e) processing only human-generated computer files by eliminating operating system files and program files; and

f) devising search terms likely to isolate the potentially relevant evidence.

2. Use a document review software tool that *you* can be comfortable with. The vendor you use may want to push its own proprietary software, or it is a reseller of some high-powered but expensive and complex document review platform.

Remember, this is *your* early assessment of what you hope will be the most relevant and most easily accessible information. Save the big guns for full-bore e-discovery later; right now, your aim is to try to get to the heart of the case to see where the major vulnerabilities or opportunities are.

Cheap and reliable review tools for you to consider are QuickView Plus, available at www.avantstar.com, and for Outlook PST and individual emails in MSG format, MsgViewer Pro at www.encryptomatic.com. Technology also exists to give you easy-to-read PDF reports of key evidence chronologically so the ESI overview can read like a John Grisham novel.[1]

3. Another useful tool for document review, though it does have quite a learning curve, is dtSearch at www.dtSearch.com, inasmuch as it has a feature called "relevance ranking" that uses an algorithm to rank search results based on the search terms you use. You can set search term results so that files are ranked in accordance to the percentage by which each file meets the search criteria.

In my experience, you can safely exclude from early case review files that have a relevancy ranking of 15 percent or less, and that often can amount to legitimately ignoring up to 90 percent of the search result "hits" you get.

4. Hire an e-discovery lawyer/technology consultant to guide and tutor you through your first forays into early case assessment of the digital evidence. The expense of using a consultant will be more than offset by the cost of your time it would otherwise take for you to set up an efficient and comfortable workflow. This person can also be your watchdog over any vendors you may wish to utilize to perform the relatively modest task of early case assessment data processing. ■

Larry G. Johnson is a lawyer in Newcastle, and has been a member of the Washington bar since 1974. He recently served on the E-Discovery Subcommittee of the WSBA Escalating Cost of Civil Litigation (ECCL) Task Force. Besides being a litigator, for the past 20 years he has served as a consultant and expert witness in e-discovery matters. He does business as Electronic Data Evidence (www.e-dataevidence.com).

[1] For more on this, see my article in the October 2015 issue of the KCBA Bar Bulletin, "What's in Your Pocket? Smartphones: A New "Safe Harbor" for E-Discovery," at *https://www.kcba.org/newsevents/barbulletin/BView.aspx?Month=10&Year=2015&AID=article1.htm*.