Metadata Strategies in Litigation:

What You Don't See Might Hurt You

By Albert Kassis

Introduction

Under Amended Rules of Civil Procedure Rule 26(f), the discovery conference requirement must now encompass a discussion of electronic discovery. The Advisory Notes further suggest that the parties should discuss whether and how metadata should be exchanged. This article discusses how metadata may be used after the hurdle of whether there is a "particularized need" is established, as some courts require.

Benefits of Metadata

Metadata have specific benefits to both sides litigating a matter. First, let's discuss the meaning of metadata, commonly defined as "data about data." The *Williams*[1] court defined metadata as: "the history, tracking, or management of an electronic document." [2]

Albert Kassis is National Director of Esquire Litigation Solutions, Hobart West. Esquire Litigation Solutions provides nationwide litigation support and technology-based document management solutions. He has advised in-house and outside counsel for Fortune 100 companies on electronic discovery issues. Mr. Kassis received his JD and BA from the University of Maryland. He is also a CPA

Metadata can include records of changes, comments, dates and other information. This information can sometimes spell the difference between winning and losing cases at trial or being forced to settle cases where there initially appeared to be little at risk.

Metadata are created by the software program in the background during normal operations. Although there are default fields captured by the program, a user can also determine which metadata will be captured. When documents or e-mails are created in the electronic environment, you can make certain that some key fundamental attributes or e-artifacts otherwise known as metadata are being captured.

Metadata can include records of changes, comments, dates and other information. This information can sometimes spell the difference between winning and losing cases at trial or being forced to settle cases where there initially appeared to be little at risk. This metadata typically is not seen unless you purposefully look for it, so it is often overlooked until there is litigation.

Different programs and versions of those programs will record different metadata, and the ability to retrieve metadata are not limited to one software provider. Most of us are familiar with Windows applications. Microsoft Word, for example, allows for the tracking of the file size, type of file and date of modification. Some of these data elements can be easily found. In Word, one can select "File/Properties" and see some of the hidden information about the document. The "General" tab displays the title, location and history. Similarly, the "Statistics" tab contains an assortment of document metrics including the number of lines, pages and words.

Metadata extraction from source documents, including MS Office specific tags, Microsoft Outlook e-mail specific tags, and Lotus Notes specific tags are some other examples. Whether you are using a Microsoft application or Lotus Notes software, rest assured that the software is creating metadata. Some standard metadata available include:

- Date Sent
- Time Sent
- Subject
- Filename
- Author
- Last Author
- File Size
- File Date
- File Time
- Modify Date
- BCC
- CC
- File Print Date & Time
- Phone Message
- Return Receipt
- Read Receipt
- Bookmark

Whether these fields may prove useful at trial or at a deposition is determined by counsel. Viewing this list of metadata in context can lead to correlations that may imply a number of potentially vital fact-specific activities.

Let's review a couple of examples. Whether someone had knowledge of a document can be material. Correlating one or more of the above metadata fields to prove document knowledge by an individual could be beneficial to a case. Recalling particular document metadata can also be used as a follow-up to questioning when someone disputes knowledge of a paper-only version.

Additionally, particular knowledge of material that was not in the finished document draft can be determined through examining changes tracked automatically by the software. Microsoft Word, for instance, allows collaborators on the same document to view each other's changes and make comments. As this document goes back and forth with the "track changes" feature active, the software captures all changes. These changes become part of that document's metadata.

"Track changes" also has a hidden text option which can keep these changes hidden when the person editing the document makes revisions. In this case both the original text and changes are tracked. Track changes metadata can reveal the timing of a particular document change, when it was made and even by whom. This may help in contract cases, for example. One particular use would be a matter involving a contract where intent was an issue.

Further, file path information can reveal where a document came from. This file path information can be used to track a document back to an individual's folder. Also, the file path can be used as a mechanism to track other relevant documents.

Consider other contexts in which metadata can be used. Metadata can establish a pattern to further a prejudice or bias proclamation. Documents may be created by someone and then revised by someone else. Let's say an employee's documents are being revised by a manager more often than documents of other employees. While this in and of itself may not prove bias, a comparison of these actions connected to other circumstances may be useful. It may indicate that this manager was not exerting the same level of oversight on other employees. The metadata may substantiate other patterns of bias.

Despite the fact that your witness or deponent may not have changed the document, that person may have printed it. Metadata in some programs is

able to capture that information. An attorney can determine when a particular file was printed, and by whom. Additionally, the specific printer that was used in many instances can also be tracked. Correlations associated with these data points can be made. If a printer is only assigned to a local user and if in fact a document is tracked to that printer, the correlation between the printing of a document and that person's knowledge of the document may be more easily made.

If the knowledge of a document, its contents or existence are not critical, possibly the date of their creation may be of relevance. For example, whether a witness or deponent feels an event is critical or not can have certain implications. If metadata were able to reveal that an electronic document was created right after an event, and the two are closely time-linked, that timing may be useful. A skillful attorney may be able to draw out a "self-perceived" criticalness on the part of the witness or deponent. It would be clear that if an event happened in the morning and someone created a document about the event shortly thereafter, the perceived urgency because of the close approximation may be easier to prove, even more so if the document were not created but were modified in close proximity to an event. Similarly, a lack of timing connection may help to disprove the lack of criticalness as well. Equally as useful is if metadata show the document was created well before the subject event took place.

At times the content of a document is not as relevant as the fact that the document was sent and then received. Use of e-mail as a delivery mechanism provides an easily-tracked trail of footprints. If a deponent or witness used e-mail as a vehicle for sending an electronic document to a recipient, the actual delivery and relationship of both sender and recipient may be easier to prove.

Tracking a "path" of a document allows one to see if your witness or deponent was part of the e-mail string, as either sender or recipient directly or blind copied. A recipient may later forward a document. Occasionally a sender of an e-mail will ask for an electronic "read" notification. This notification can take on several forms. In its simplest form when a recipient receives an e-mail and opens it for viewing even in preview mode an electronic message will go back to sender indicating that the message was "read." Whether it was indeed actually read word for word is another matter.

Let's consider activity around the document. Typically when meetings are scheduled or calendared, relevant meeting documents are appended or attached to the actual invite. Having an "invite" appear within a deponent's or witness's calendar may provide document knowledge. At times one may delete documents from folders and even delete e-mails containing those documents. Calendar invites containing these appended documents might be overlooked and therefore remain long after. Looking for calendaring events in the course of discovery may yield useful information. Metadata correlating an invite event to an individual can be mined for relevant documents.

Metadata can also help with timelines. Dates associated with both e-mails and document activities can provide date guideposts that are useful. This usefulness falls outside the content of the e-mail or document. Occasionally timelines can reveal document or e-mail gaps for the purpose of arguing an incomplete production in discovery.

Tripping Up a Deponent

Counsel should also be leery of how metadata can trip up a deponent. Some examples include:

- Excel spreadsheets may display the name of an author who is not the deponent.
- Electronic documents may contain critical formulas that cannot be explained by the witness or deponent despite the fact they are addressing data within the document.
- E-mails in electronic form should contain specific addresses as opposed to just a name with no domain address. This may be an issue with common names in large corporations.

Conclusion

Overall, metadata and its uses will continue to evolve as software changes. Service providers have the arduous task of accommodating software and e-mail changes to ensure any captured metadata are extracted and made available for review. Counsel will continue to utilize metadata in depositions and trial where the captured data can prove or disprove an argument.

1. *Williams v. Spring/United Mgt. Col,* 230 F.R.D. 640 (D. Kan. 2005).
2. *Williams v. Spring/United Mgt. Col,* 230 F.R.D. 640, 646 (D. Kan. 2005).