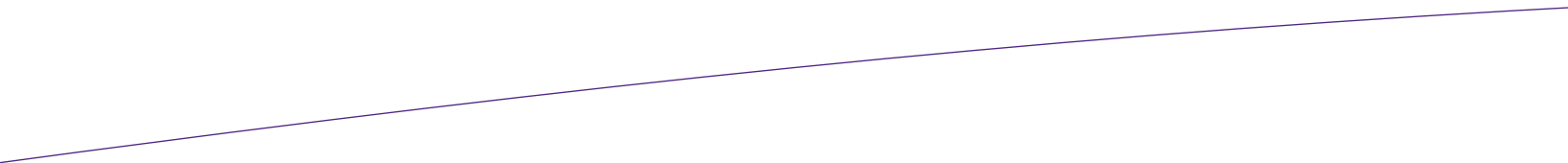




Embedded Information in Electronic Documents

Why Metadata Matters



Lawyers practicing in the electronic age cannot ignore a new source of evidence: metadata. Metadata (also known as “embedded data”) literally means “data about data.” It is a critical component of electronically stored documents. Lawyers can use it to bolster their own cases, streamline document review, and get the complete story of their adversaries’ documents.

Software programs embed various categories of metadata in the documents users create. Metadata describes how, when, and by whom an electronic document was created, modified, and transmitted. This administrative information assists data retrieval—and reveals a document’s history.

Metadata represents a crucial difference between electronic and printed documents. All the information in a paper document is displayed on its face. Not so with electronic documents. Electronic documents carry their history with them. Paper shows what a document said or looked like—metadata tells where the document went and what it did.

Growing Importance in Litigation

As lawyers become aware of metadata as a source of evidence, it gains importance in litigation. Recognizing its evidentiary value, more lawyers are requesting it from opposing parties as well as using it as a resource in making their own cases. Before producing documents, a review team needs to be aware of and prepared to confront any embedded information that might harm a client’s position. Lawyers can expect at some point to face a request—or order—to produce metadata.

Significantly, metadata is not a separate document, but an integral part of the document it describes. One court, rejecting the argument that printouts adequately represented emails, described emails without their metadata as “dismembered documents indeed.”

Recent advances in technology make preserving and viewing metadata easier. Expectations are changing about what must be produced. New tools and increasing appreciation of metadata’s evidentiary value drive its growing importance in litigation. How might metadata matter to your case?

Types of Metadata

For lawyers’ purposes, one of the most important examples of metadata is that embedded in email. Email prevails in communications, so it follows that many cases now feature email evidence.

An email carries information about its author, creation date, attachments, and identities of all recipients, including those who received a cc or bcc. As email “conversations” take place, the email accumulates a conversation thread: replies to the sender, to other recipients, and forwards. That history becomes part of the message’s metadata, allowing reviewers to trace a message or reconstruct an email conversation.

Metadata also connects attachments to emails. When email is a vehicle for transmitting other documents, such as word processing documents, spreadsheets, or presentations, links to those attachments are part of the email’s metadata. Preserving these links means that a reviewer can tell what document, and which version of it, was attached to a particular email.

Regrettable emails have received a good deal of press attention, and many lawyers have stories to tell about how emails have factored in to their cases. But emails are just one example of documents that hold metadata

evidence. Information embedded in other file types may include document names, file save locations, authors, and editors. Previous edits to a document may be accessible. “Track changes” features reflect modifications by each recipient. CAD drawings can show who crafted previous versions of a design, and when.

All of this information was unavailable to lawyers in the days of paper storage. When the background of a document was disputed, the answer was to depose witnesses. With electronic information, litigators don’t have to rely on or debate witnesses’ memories. Metadata settles factual disputes about a document’s history: the document tells its own story. Consider some examples.

In one case, a plaintiff claimed that she was discharged in retaliation for making a sexual harassment complaint. To refute the allegation of retaliatory motive, the defendant produced a memo, dated before her sexual harassment complaint, that included the plaintiff on a list of employees to be let go in a planned seasonal layoff. She claimed that the memo was fabricated in response to the litigation. The memo’s metadata confirmed its date of creation, prior to her complaint.

Another terminated employee fabricated an email to suggest that a manager with whom she had a romantic relationship had made the decision to terminate her. Metadata exposed the plaintiff herself as the document’s author.

Yet another plaintiff contended that the defendant had improperly omitted some emails from production. The defendant refuted this claim by reconstructing a chain of emails, establishing that it had produced all that was requested.

Often, the heart of an email is not its text, but its attachments. If documents are reviewed in printed form, those relationships are difficult to reconstruct. Metadata can maintain the links between emails and attachments, including which version of a document was attached to which email. When a dispute arises over how various recipients changed a document, or what information a witness had at a given time, metadata often resolves the issue.

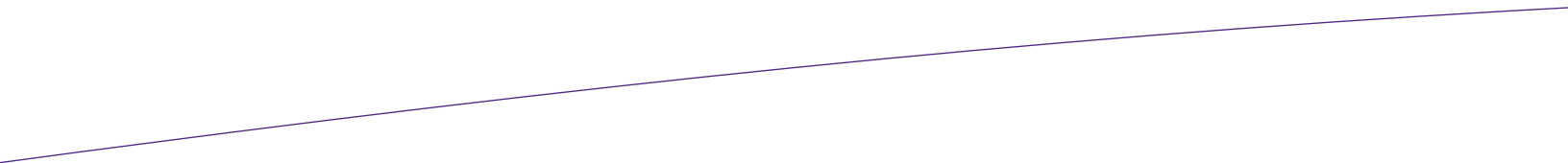
In any factual dispute involving knowledge of particular information, metadata is a great resource. It reveals the identities of recipients, and when they received and opened a document. In issues such as fraud, negligent misrepresentation, or insider trading—when it can be crucial what a witness knew, and when—metadata can provide invaluable evidence.

When parties exchange different versions of a document using a “track changes” feature, the changes become part of the metadata. This information can be critical in situations such as a contract dispute involving the parties’ intent in negotiations.

Metadata is a trove of information about whether an adversary has properly preserved documents in the face of litigation. It reveals when a document was last modified or accessed. If documents are missing, it can reveal when they were deleted.

Streamlined Document Review

In addition to these uses in factual disputes, metadata can be a valuable resource in the document review process, whether in litigation or in mergers and acquisitions practice, where lawyers often face government



demands for production on tight timelines. It allows electronic searching of various fields: lawyers can quickly locate keywords and filter searches by other criteria, including a document's source, the name of a witness, a time period, or a subject line. These search capacities make it possible for reviewing lawyers to quickly sort even millions of pages, eliminating superfluous documents and filtering an otherwise unmanageable volume of documents into a workable set for review and production.

File path information that reveals where a document came from (what file or source, for example) may help locate other pertinent documents. Lawyers reviewing for attorney-client privilege can quickly detect the identities of document authors and recipients. If there is an allegation that purportedly privileged material was in fact shared with individuals outside the scope of the privilege, the email's metadata will show recipients—including anyone who received a bcc.

Metadata can also reveal the actual destination of an email, rather than just the name in the address field. This information is important for a witness who uses multiple display names, or an email alias. User names and email aliases may not be meaningful to a reviewer without the identity of the associated person. For example, in the Microsoft antitrust litigation, Bill Gates' emails became an important source of evidence. He received intra-company emails under a number of different names. Metadata would capture all those messages by tracking the full email address, not just the "friendly" name appearing in the address field. Distribution lists also may be meaningless without this capability. A reviewer could not otherwise identify, for example, recipients of an email sent to a group distribution list, like "Sales," or "ExecutiveTeam."

It takes little imagination for a lawyer to see the value of metadata, whether in requesting documents, building a client's own evidence, or simply sifting through masses of documents on a deadline. It accelerates review and proves facts that might otherwise generate disputes and further discovery. But lawyers need to be sure that their own document review tools are not compromising this information. Metadata can only be captured, accessed, and viewed through electronic means. This makes proper electronic document processes essential.

Preserving Metadata

Some methods of document review fail to account for and preserve metadata. If a document is printed in the review and production process, its metadata is lost. A printout displays only the face of the document—not its embedded history.

Many lawyers believe they are conducting "electronic discovery" when in fact they are merely working with electronic images of documents. The process of scanning and coding documents into a database does not capture original document metadata. Additional software can allow limited electronic searching, but the original information embedded in the document is lost. Likewise, subjectively coding a database to recognize certain terms does not restore the metadata lost in the reduction to paper. It is a poor substitute for the original electronic document.

The ability to see layers of information behind the face of a document has obvious implications for litigators, whether a party is ordered to produce it or uses it to its own advantage. Lawyers must take care that their review methods capture this essential information.

The Discovery Experts: Industry Relations

LexisNexis Discovery Services has the right consulting and technology choice for every discovery need. Top law firms, corporations and government agencies rely on the LexisNexis® products and services, Applied Discovery®, Concordance™, and Hosted FYI™, to meet their discovery obligations on time, accurately and cost-effectively. Services include records management consulting, data collection, forensics, media restoration, data filtering, data processing, review and document production in the format that each matter requires. The Industry Relations team works to educate the legal community on the continually evolving case law and technology of electronic discovery.

For more information or to contact the experts, please visit lexisnexis.com/discovery.

