

# Alternative Privilege Log Techniques in an E-discovery World

BY ELIZABETH T. TIMKOVICH AND MEGHAN A. O'DONNELL

Any litigator involved in the collection, review, and production of documents in today's world of electronically stored information (ESI) has likely dealt with the costly and time-consuming "morass" of e-discovery.<sup>1</sup> Thanks to the ability of people and companies to store increasing amounts of information using numerous types of electronic media, the volume of electronic documents subject to discovery has exploded in recent years. This is especially true for large class actions, antitrust investigations, and other information-heavy disputes. Many in the legal community have written on the need to improve and streamline e-discovery rules and techniques for collecting and reviewing ESI. There is another costly by-product of e-discovery, though, that also screams to be addressed: preparation of the privilege log.

Typically, a privilege log consists of a spreadsheet or table identifying responsive documents that have been withheld from production as privileged by listing, at a minimum, each document's custodian, author, addressees, creation or last modification date, subject matter, and basis for privilege (e.g., attorney-client privilege, work-product immunity). Thanks to modern e-discovery software, some of these identification fields—i.e., custodian, last modification date, and (for some types of documents) author and addressees—can be automatically populated from each electronic document's metadata.<sup>2</sup> The remaining fields, however, must typically be manually filled by the attorneys preparing the privilege log (the "privilege loggers"). For example, for an email chain between an attorney and a client regarding an ongoing class action dispute, a privilege logger might have to type the following phrases into the respective privilege log fields: "email chain between attorney and client, requesting and providing legal advice of Attorney Smith regarding instant litigation."

This manual data entry can be extremely time-consuming (not to mention mind-numbing), especially in cases where large numbers of documents are being withheld and individual privilege descriptions must be entered for each. And because attorneys are typically the professionals tasked with privilege log preparation, drafting and revising log entries is extremely expensive to the client. As a result, it is not unheard of in certain discovery-heavy disputes for the costs of preparing a large commercial party's privilege log to rival or even surpass the costs incurred in conducting the underlying review of the collected documents. It is clear, therefore, that many litigants would greatly benefit from an alternative to the traditional, manually constructed privilege log.

## Proposed Alternatives

Provided all parties agree, the following proposed alternatives to the traditional privilege log format and content (at least with respect to ESI) could result in a quick, easy, and relatively inexpensive privilege log. For example, litigants could agree to exchange privilege logs identifying withheld electronic documents solely by specified portions of the documents' already-existing metadata. A typical electronic document's metadata identifies, among other things: the custodian, document type (e.g., email, Word document, Excel spreadsheet, etc.), date last modified or sent, file name, and, if an email or email chain, the author and addressees in the most recent email. If the parties can agree to populate their privilege logs with such inherent metadata and forego additional descriptions requiring manual data entry, creation of each privilege log should be as simple as exporting the desired metadata fields into an Excel spreadsheet. Most e-discovery review tools on the market today—such as Kroll Ontrack Inview, CaseCentral, Concordance—allow such data exports to be very easily accomplished and readily accessible.

Should the parties desire more information than is provided in inherent metadata, the following additional steps could be taken to add category and/or keyword information to the log (while still avoiding manual data entry). If documents were categorized during electronic review, then metadata fields could be created—depending on which e-discovery software is being used—that would identify which substantive categories were selected for each document. Also, litigants could run keyword searches against the pool of withheld documents to identify those containing specific names (e.g., of attorneys), privilege-indicating legends such as "attorney-client," or other significant words or phrases. Metadata fields could be created for the documents identified in each search, reflecting the applicable search term(s) found therein. The identification of such keywords or phrases in the withheld documents could be useful not only to justify or challenge privilege claims, but also to more easily identify those documents likely or unlikely to have especial relevance to the litigation.

This technique of searching out and providing additional descriptive data based on keyword searches will certainly require more time and review-tool expertise than the simple exportation of inherent metadata described in the preceding paragraph, but it is still a much faster and less costly alternative to the manual privilege log that is currently used wide and far.

## Caveats

Of course, use of the alternative privilege logging techniques proposed here will not work well for every kind of case (e.g., cases in which the bulk of documents to be reviewed and produced consist of paper documents rather than ESI), and many log entries are bound to be challenged. For example, log entries relying on inherent metadata alone may not provide accurate privilege descriptions for redacted documents or for email chains. (As previously noted, the inherent author and addressee metadata for email chains captures only the identities of those individuals listed in the topmost email of a chain.) Litigants may wish, therefore, to request additional privilege log requirements, beyond use of inherent metadata, for these or other special types of documents. Also, if the proposed search term technique for supplementing inherent

metadata is pursued, an opposing party may challenge the log entries for documents that do not contain any of the searched-for terms.

Such potential challenges should not, however, dissuade parties from pursuing an alternative privilege log arrangement. After all, even traditional, more narrative privilege logs are subject to frequent challenge. Each party could agree, at a minimum, to produce as its primary privilege log a metadata-based log and

to then supplement that log with additional requested data (perhaps in the form of more traditional narrative statements) for those documents specifically challenged by its opponent. The parties might also grant each other a “quick peek” at the challenged documents.<sup>3</sup> If nothing else, this approach should greatly cut down on the number of withheld documents for which traditional narrative logging is required. Litigants could drill down on just those documents—perhaps those with categories or search hits indicating a high degree of relevance—for which additional information is actually desired. Litigants might be most willing to agree to such an arrangement where all parties to the dispute wish to avoid high discovery costs, or where expedited discovery is required.

## Rule 26 Is Not Violated

Litigants’ use of the proposed metadata-based privilege logging techniques should not violate Rule 26 of the Federal Rules of Civil Procedure pertaining to discovery and assertions of privilege. The pertinent section of Rule 26 requires

only that a party make privilege claims expressly and that it describe the withheld material well enough to permit its opponent to test the privilege claim’s validity.<sup>4</sup> The rule does not specify the precise level of detail required for an express claim of privilege, nor does it mandate the parameters of a “log.” Instead, it states the following:

When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must: (1) expressly make the claim; and (2) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.<sup>5</sup>

Moreover, the Notes of the Advisory Committee on the 1993 amendments to Rule 26(b)(5) strongly indicate that metadata-based privilege logs would satisfy Rule 26. The Notes state:

The party must also provide sufficient information to enable other parties to evaluate the applicability of the claimed privilege or protection. . . . *The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection. Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.*

Furthermore, the Notes of the Advisory Committee on the 2006 amendments helpfully explain:

Parties may attempt to minimize [e-discovery] costs and delays by agreeing to protocols that minimize the risk of [privilege] waiver. They may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection—sometimes known as a “quick peek.” The requesting party then designates the documents it wishes to have actually produced. . . . *Other voluntary arrangements may be appropriate* depending on the circumstances of each litigation.<sup>6</sup>

From the previous excerpts, it is clear that no federal procedural rule prohibits use of the alternative privilege log forms proposed by this article, although parties considering the use of such logs are still advised to check their local court rules. Use of metadata-based privilege logs for withheld electronic documents could save attorneys and their clients

The use of metadata-based privilege logs for withheld electronic documents could save attorneys and their clients considerable time and money.

considerable time and money, and should, therefore, be considered by parties seeking to reduce their e-discovery costs.

*Elizabeth T. Timkovich and Meghan A. O'Donnell are attorneys with Hunton & Williams LLP, practicing, respectively, in Charlotte, North Carolina, and Richmond, Virginia.*

---

1. See, e.g., Interim Report on the Joint Project of The American College of Trial Lawyers Task Force on Discovery And The Institute for the Advancement of the American Legal System (Aug. 1, 2008) at 3 (“Electronic discovery . . . is described time and time again as a ‘morass.’ . . . The bigger the case, the more the abuse and the bigger the nightmare.”).

2. Commonly referred to as “data about data,” metadata

tracks and reveals data about document attributes, such as name, size, type, where it is located, and ownership. Metadata for an email, e.g., is “data stored in the email about the email,” such as addressees and received date. Metadata for other electronic documents reveals “[p]roperties about the file stored in the file, as opposed to document content,” including author, creation, and revision dates. The Sedona Conference Glossary: E-Discovery & Digital Information Management, Second Edition (Dec. 2007).

3. See FED. R. EVID. 502.

4. See FED. R. CIV. P. 26(b)(5).

5. *Id.*

6. *Id.* (emphasis added).