The Legal Intelligencer

Privilege Logs: Strategy, Best Practices and Practical Advice

In this article, we provide an overview of the different types of privilege logs; lay out best practices for negotiating ESI or privilege-log protocols; discuss what to do if an ESI or privilege-log protocol has not been entered in a matter; consider practical uses of technology to generate privilege logs; and address the inadvertent production of a privileged document.

L-R: Leonard Impagliazzo, Bansri Mehta McCarthy and Tara S. Lawler of Morgan Lewis & Bockius. Courtesy photos

By Bansri McCarthy, Leonard Impagliazzo and Tara Lawler

December 27, 2022

In this year's final installment of our series on e-discovery basics, we delve into the world of privilege logs. Gone are the days when a lawyer would print out documents and prepare a privilege log by drafting individual descriptions—one privileged document at a time. Leveraging the latest technological tools, today's eData lawyers are as sophisticated and efficient in preparing privilege logs as they are in all other phases of discovery. Privilege-log planning should begin well before the first privileged document

is logged. In fact, privilege-log strategy should be considered at the outset of a matter and included in early meet-and-confers with opposing counsel about the discovery process. In this article, we provide an overview of the different types of privilege logs; lay out best practices for negotiating ESI or privilege-log protocols; discuss what to do if an ESI or privilege-log protocol has not been entered in a matter; consider practical uses of technology to generate privilege logs; and address the inadvertent production of a privileged document.

Privilege Log Types

Not all privilege logs are identical; they can vary widely in detail, scope and burden. The Federal Rules of Civil Procedure do not use the term "log" or otherwise spell out logging procedures. Instead, Rule 26(b)(5)(A)(ii) requires a withholding party to "describe the nature" of withheld documents "in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim." In the absence of clearly defined requirements, three types of privilege logs have emerged.

Traditional privilege logs contain an individualized description for the privilege asserted on each document and are universally accepted by courts. Technology can be leveraged to extract metadata for the objective fields in a traditional privilege log, but these logs require distinct descriptions for each logged document. While the distinct descriptions allow the receiving party to evaluate the privilege basis for each document, traditional privilege logs are burdensome to prepare in both time and expense, particularly in matters with large volumes of privileged documents. The burden of preparing a traditional log is not always proportional to the need, as not all withheld documents require privilege descriptions to adequately show the reason for the withholding. In addition to traditional logs, there are two

alternative types of privilege logs. Metadata privilege logs are the most expedient and inexpensive of privilege logs, comprising an export of agreed-upon metadata that is available for logged documents in the review database.

Metadata privilege logs can be created expeditiously, resulting in significant cost savings in preparation (especially in matters with a large volume of logged documents). The disadvantage of metadata privilege logs is the possibility that certain documents may lack sufficient metadata to properly assess a claim of privilege (e.g., hard-copy privileged documents), and it may be difficult to gain insight into the privilege basis for email threads. To overcome these potential issues, eData lawyers should consider adding a provision to the privilege log protocol allowing for supplementation, upon reasonable requests by the receiving party, of additional information for individual documents and types of documents.

Categorical privilege logs group documents with similar privilege bases as a unit on the privilege log. Each category represents one entry and provides a single description for all privileged documents contained within that category, as well as metadata representative of all documents within that category (e.g., document date would include a date range encompassing the dates of all documents within the category; recipients would include all recipients of all documents within the category). Withholding parties can optimize efficiency and organization by grouping documents with similar bases together, and receiving parties can assess privilege claims at a high level based on the parties involved and the general subject matter of the category. Bear in mind that categorical privilege logs are more time-consuming to prepare than metadata privilege logs, and it can be difficult to categorize documents that contain unique privileged content. While more

costly than metadata privilege logs, categorical logs do represent time and cost savings over traditional privilege logs.

Privilege Log Preparation and Planning

eData lawyers should begin planning for the privilege log well in advance of generating the log, ideally during meet-and-confers and during ESI or privilege-log protocol negotiation.

It is essential that eData lawyers know their jurisdiction's privilege-log requirements. As mentioned above, the Federal Rules of Civil Procedure do not set out specific logging methods, allowing local court rules to fill in the gaps. For example, New York state courts prefer the use of categorical privilege logs "to reduce the time and costs associated with preparing privilege logs." In preparing categorical privilege logs, "parties are encouraged to utilize any reasoned method of organizing documents that will facilitate an orderly assessment as to the appropriateness of withheld documents in the specified category." See N.Y. Comp. Codes R. & Regs. tit. 22 Section 202.70.11-b. Contrast that with the U.S. Court of Appeals for the Seventh Circuit's Electronic Discovery Pilot Program, which prefers metadata privilege logs and says that metadata logs should provide "as much objective metadata as is reasonably available (e.g., document control number, date, author(s), recipient(s), file type, etc.) and an indication of the privilege and protection being asserted," as well as "a description of any categories of ESI and documents that the withholding party asserts are privileged or protected and the reasons for asserting that individual review of the category is not worth the time and expense necessary to do so." Jurisdictional guidance may obviate the need for negotiation on certain points and will save parties significant time and cost over having to redo a privilege log that does not meet a court's requirements.

Negotiating Privilege Log Protocols

In the absence of jurisdictional guidance on privilege logs, memorializing the particulars of privilege logging in an ESI or privilege log protocol allows parties to ensure that they will receive the information they deem necessary to assess the withholding party's claim, as well as plan their own privilege review in the most efficient and cost-effective manner possible. A well-thought-out protocol on privilege logging can help avoid lengthy and costly discovery disputes downstream. The protocol should contemplate an array of items relating to the form and substance of the privilege log, as well as remediation processes for inadvertent disclosure of privileged material.

Firstly, and perhaps most importantly, eData lawyers should negotiate the type of log that will be prepared: a traditional log, a metadata log or a categorical log. In some cases, it may be appropriate to use a hybrid approach. For instance, a matter that involves large volumes of ESI and hard-copy documents may be a candidate for the use of a categorical or traditional log for the hard-copy documents in combination with a metadata log for the ESI.

After agreeing to a privilege log format, eData lawyers should contemplate the fields to be included in the privilege log. At a minimum, privilege logs should contain the document date, parties involved (to/from/cc/bcc), the privilege claim, and a brief description of the withheld material (if applicable in the type of log). Parties may want to request and provide additional metadata to help in assessing privilege claims, especially in metadata logs which do not contain descriptions. Helpful fields may include custodian, Bates numbers, email subject, file name, author, date last modified and who last modified it.

Parties should discuss the types of privileges they expect to encounter in their data. The two most common types of privilege protection are attorney-client privilege and attorney work-product privilege. However, other protections may be applicable, such as federally authorized tax practitioner privilege (in tax matters before the DOJ and IRS) or common-interest privilege (as an exception to waiver of privilege). These should be described in detail in the protocol.

It may also be worthwhile to negotiate the exclusion of certain categories of documents from privilege logs to reduce cost and burden. For example, redacted documents are often excluded under the rationale that the receiving party can glean the privilege assertion of the withheld material from the produced portions of the document (e.g., recipients, subject line and document date). Privileged documents generated after the filing of the complaint are a common exclusion because they are considered presumptively privileged, and there are limited benefits from seeing them on a log. Communications to and from outside counsel are another worthwhile exclusion because they are also presumptively privileged.

Similarly, eData lawyers should consider the benefits of one entry per fully withheld family versus one entry per document within a family. Logging entirely withheld families as one entry minimizes the size of the log, particularly in cases with large volumes of privileged documents, and reduces the burden of preparation on the producing party, as well as the burden of assessment on the receiving party.

Finally, parties should discuss the timing and production of the privilege log. Rolling logs are often inefficient, requiring corrections and reproductions based on newly discovered information. If possible, agree to produce one

privilege log within a reasonable timeframe following substantial completion of document production (e.g., 30-60 days) and avoid agreeing to serve privilege logs at the time of production. Serving privilege logs alongside productions is logistically burdensome and may compromise the quality and accuracy of entries. Service of one privilege log following substantial completion is preferred because it ensures that parties are receiving both the most up-to-date production content and the most accurate privilege log possible.

When There's No Logging Agreement

What should parties do when the court does not provide guidance, and privilege log specifics have not been negotiated in advance? There are best practices to follow in preparing a privilege log. Most importantly, always prepare a privilege log. Failure to provide a log could result in the waiver of privilege or sanctions.

Although parties will often default to providing a traditional privilege log when no logging protocols are in place, consider starting with a metadata privilege log to limit expense and provide the basis for withholding the privileged documents in an expedient manner. Be transparent with opposing counsel and offer to supplement entries, if needed, within a reasonable timeframe. The supplement may include additional metadata, categorical entries, traditional privilege log descriptions, or some combination thereof. In preparing the privilege log, eData lawyers should focus on the substance and accuracy of the privilege log using the suggestions below. The format can be adjusted or supplemented upon further discussions with opposing counsel.

Practical Uses of Technology in the Preparation and Quality Control of Privilege Logs

The technological tools that eData lawyers rely on for relevance reviews are likewise indispensable to privilege reviews and in the preparation of privilege logs. For example, eData lawyers should use email threading technology to verify differing calls within an email thread, as well as duplicate document comparison to check differing calls on duplicate documents. While it is common to have differing privilege calls within threads or on identical documents, due to family relationships, these quality-control checks are a fundamental step in ensuring that the privilege log will be accurate, and that privileged material is not inadvertently produced. eData lawyers should also utilize technology to identify redacted documents, as well as partially privileged documents. This ensures that all documents intended to be partially withheld contain the appropriate redactions and that documents redacted for nonprivileged reasons do not mistakenly end up on the privilege log.

Another key software tool that eData lawyers should leverage is name normalization functionality. Name normalization reduces confusion and speeds the receiving party's review by accounting for name variations that are commonly present in ESI (e.g., Doe, John; John Doe; and JDoe@Company.com).

Last but not least, eData lawyers should strongly consider using drop-downs or prepopulated pick lists to help draft consistent descriptions on matters with a large volume of privileged documents. When preparing traditional privilege logs, consistency in descriptions is paramount.

Small variations in language style and formatting are magnified when they appear next to each other in rows upon rows of privilege entries. Using drop-downs or pick lists to create a privilege log palette, much like a relevance review palette, is an essential tool in preparing a clean, professional privilege log for matters where multiple eData lawyers will be drafting descriptions.

Protecting Client Privilege in the Event of Inadvertent Disclosure

In this era of voluminous data, inadvertent production of privileged material is not uncommon, even when robust privilege review protocols and quality-control checks are in place. It is imperative to include a 502(d) provision in the ESI or privilege protocol for such instances. Federal Rule of Evidence 502(b) protects against waiver of privilege as a result of disclosure but requires that the disclosure was "inadvertent; the holder of the privilege took reasonable steps to prevent disclosure; and the holder promptly took reasonable steps to rectify the error."

However, the rule does not define "inadvertent," what a reasonable privilege screening methodology entails, or what constitutes prompt and "reasonable steps to rectify the error." Relying on Rule 502(b) to protect a client's privileged material can result in lengthy and costly motion practice if the privilege review process or clawback timing is challenged. Federal Rule of Evidence 502(d) allows eData lawyers to enter into their own clawback agreement without being subject to the proof requirements of 502(b). It should be noted, however, that some courts have refused to enforce 502(d) agreements where the parties did not consider 502(b) standards. As such, while a 502(d) order is preferred, parties should ensure that they are taking

reasonable steps to prevent inadvertent production of privileged documents and be prepared to show the steps taken, if asked by the court.

Preparing a privilege log can be a daunting endeavor, but the exercise can be made infinitely more manageable by strategizing early in the discovery process and planning for pitfalls. eData lawyers should consider the potential volume of privileged documents and the type of privileged content they expect to encounter, as well as the technological tools available to facilitate the generation of a privilege log, during the meet-and-confer and ESI or privilege-log protocol stage. Doing so can encourage parties to arrive at a mutual understanding of expectations, reduce challenges to the privilege logs, control costs and minimize avoidable motion practice.

Morgan Lewis & Bockius partner **Tara Lawler***'s practice focuses on e-discovery, information management and data privacy. Associate* **Bansri McCarthy** *has a practice that focuses on technology and e-disovery and associate* **Leonard Impagliazzo***'s practice focuses on e-discovery, information management and data privacy.*

Reprinted with permission from the December 27, 2022 issue of The Legal Intelligencer © 2022 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved.