

Tip of the Month



Managing the Risks & Costs of the Production of Private or Confidential Information: Redaction & Production Strategies

Scenario

A financial services organization is a party to a litigation in which plaintiffs are seeking information concerning business practices that impacts a number of the organization's customers. The organization does not want to provide private and confidential information about the organization's customers, particularly those not impacted by the alleged business practice. Some of this information may be protected by various federal and state laws, and some is not necessary for the prosecution or defense of the litigation. But that private and confidential information is intermingled with responsive non-private, non-confidential information and is contained in a variety of data formats, including very large spreadsheets. The organization is evaluating its options for protecting this private and confidential information while at the same time complying with its discovery obligations and controlling its costs.

How Electronic Data May Alter the Balance of Risks & Costs Associated with Redactions

Organizations are regularly challenged to balance their need to comply with discovery obligations and their desire to control discovery costs and protect against the unnecessary disclosure of private or confidential information. However, the proliferation of electronic data sources, coupled with the sheer volume of information contained within those electronic data sources, has had a profound impact on the costs of controlling disclosure. Historically, litigants have addressed the problem by redacting the private or confidential information prior to production: the documents in question are "TIFFed" (i.e., creating an image of the electronic document), the private or confidential information is manually redacted and then the documents are produced.

But while manual redaction of a few hundred or few thousand simple documents, like Word or hard copy documents, may be feasible and cost-effective in some instances, manual redactions of tens of thousands documents, especially when it involves more complex data types like spreadsheets, present more challenges. In addition to the increased time and costs involved with the redactions—as well the costs associated with TIFFing data types that are often produced in native format (like spreadsheets)—more complex data types often lose significant functionality when converted to TIFF format. Increasingly, the time and costs involved with attempting redactions on a large scale are prohibitive and often offer little if any benefit to the resolution of the legal matter.

Consider Whether a Court Order is Sufficient

There is a temptation under these circumstances to simply enter into a stipulated confidentiality agreement, have the agreement so-ordered by the court and produce any private or confidential information (including non-responsive information), with the expectation that the so-ordered

confidentiality agreement will suffice. The requesting party is, and certainly most courts are, likely to support this approach. And in some instances, a court-ordered confidentiality agreement may very well be the sufficient to address an organization's concerns.

Yet in other instances, the protections provided by a court order may not sufficiently address risks to the producing party. Those risks include: (i) the potential negative impact to the organization's reputation or customer relationships if it becomes known that the organization is willingly producing non-responsive private or confidential information in response to legal requests; (ii) the ongoing risk that the organization may be liable for a data breach if the receiving party or its counsel violates the confidentiality agreement or experiences its own data breach; (iii) the potential for additional legal obligations to provide notice or obtain consent before providing such information; (iv) the business concerns with producing proprietary information to a competitor; and (v) the strategic concerns associated with producing non-responsive information that may be used against the organization in other contexts. Thus, whether a court-ordered stipulated confidentiality agreement offers sufficient protection in a particular case, as well as an organization's options if the protections are considered insufficient, should be carefully considered by the organization and its counsel.

Be Aware of the Pitfalls of Native Redaction

TIFFing documents for production, especially spreadsheets, may cause difficulties both with the redaction process and with understanding the data itself. As a result, many e-discovery vendors are working to develop tools that would allow the redaction—or removal—of private or confidential information from native documents (either manually or automatically) in a forensically sound manner. This may be a viable option in some cases. However, organizations and their counsel must keep in mind that these tools, like any tools, must be tested and vetted in each case to determine whether the tool is effective for the data type, complexity and volume at issue. Some of the challenges to keep in mind:

- *Improved Efficiency.* Native redaction tools may address one problem, i.e., avoiding costly TIFFing that makes redacting and understanding the document more difficult, but not other burdens associated with manual redaction. For example, individual reviewers may still need to conduct a comprehensive review of each cell to locate and apply the native redaction. Consider whether the tool under consideration addresses the organization's particular redaction concerns.
- *Testing Data Types.* Special formatting (such as formulas, links, pivot tables, etc.) may pose problems that need to be addressed on a document-by-document basis, even with an otherwise automated process. And even when data is removed from the visible portion of a native document, that data may still exist within the non-visible portion of the documents, such as in a cache. Conducting a thorough test on different types of data that may be subject to the review will help to determine if the native redaction tool is effective for your data.
- *Audit Trail/Documentation.* Native redaction or removal may involve altering the document itself. And in removing information from a document, it may be difficult, or impossible, to maintain the natively redacted document in the exact same format/arrangement in which it existed on the organization's system or as an attachment to an email (i.e., hidden columns, rows and filters). Evaluate whether there is sufficient documentation of the native redaction process to maintain an appropriate chain of custody.

Consider Creative Negotiation Strategies

Ultimately, the most effective production strategies may be aggressive negotiation and creative problem solving. For such a strategy to be effective, an organization and its counsel must be

prepared to demonstrate the burden imposed by traditional redactions, the need to maintain the privacy or confidentiality of the data at issue and the viability of the alternative solutions. Plaintiffs or regulators may be willing to cooperate on mutually agreeable solutions, and courts may be more willing to support alternative production arrangements, if they understand the nature of the problem and the data at issue. Some potential strategies include:

- *Understanding the Information Sought.* Information in large, complex documents, such as spreadsheets, is often generated from a central repository, such as a structured database. If that is the case, consider whether the information sought may be generated from that central repository in a form that excludes the private or confidential information. Be prepared to explain that the information sought may be provided in a consolidated, easy-to-understand format and to provide of substantive information to support the explanation.
- *Limit the Scope.* In some instances, the requesting party or the court may not require the production of *all* documents containing private or confidential information. Instead, the production of a limited number of sample documents with redactions of the private or confidential information may suffice. Be prepared to provide the requesting party with the opportunity, under controlled circumstances, to review the types of documents at issue in order to assist them in evaluating which samples must be produced.
- *Secure Production.* Consider “producing” the data to the plaintiff or regulator for review in native format via a secure platform controlled by the organization. While this approach does reveal private or confidential information to the requesting party, it may be structured to prevent downloading or dissemination of the information. The requesting party may then seek the production of a limited number of specific documents that will actually be used in the litigation in an agreed-upon format.

New discovery challenges often require new discovery strategies. And rarely, if ever, does one strategy work for every legal matter. By carefully assessing both the business and legal concerns associated with the potential production of private or confidential data in the context of each legal matter, an organization may be able to manage the risks and costs associated with the prospect of voluminous redactions of electronic data.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown’s [Electronic Discovery & Records Management](#) practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

If you would like to be informed of legal developments and Mayer Brown events that would be of interest to you please fill out our [new subscription form](#).

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the “Mayer Brown Practices”). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe – Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. “Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

IRS CIRCULAR 230 NOTICE. Any tax advice expressed above by Mayer Brown LLP was not intended or written to be used, and cannot be used, by any taxpayer to avoid U.S. federal tax penalties. If such advice was written or used to support the

promotion or marketing of the matter addressed above, then each offeree should seek advice from an independent tax advisor.

This email and any files transmitted with it are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Mayer Brown LLP, 71 S. Wacker Drive, Chicago II, 60606, Tel: +1 312 782 0600

© 2013. The Mayer Brown Practices. All rights reserved. This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

[See our privacy policy and important regulatory information.](#)