

Communication Is the Key to Avoiding e-Discovery Pitfalls

As the volume of documents stored electronically continues to grow (without apparent limit), electronic discovery (“e-discovery”) has created new challenges for litigants.

Originally published in *The National Law Review*
Reproduced with permission

Written By:
Valarie Hays
William E. Meyer Jr.

As the volume of documents stored electronically continues to grow (without apparent limit), electronic discovery (“e-discovery”) has created new challenges for litigants. The time during which the discovery stage of litigation was dominated by manual or paper production is over. In fact, “99.9 percent of information created is created digitally. . . . More than 70% of that information is never printed.”[1] Courts and litigants have struggled to deal with these challenges, and the solutions (not to mention the “rules of the game”) are still evolving. This much, however, is certain – litigants’ vulnerability to time-consuming, distracting, and costly e-discovery disputes, and the discovery of damaging evidence, will increase. Minimizing those vulnerabilities by means of education, planning, and communication will be in everyone’s best interest.

Communication During the Identification, Preservation, and Collection of Electronic Discovery Is Important

As courts and opposing counsel become more sophisticated and knowledgeable about e-discovery issues and computer search capabilities, it has become important that legal counsel engage in discussions with their clients who are involved in litigation disputes to determine where their potentially relevant Electronically Stored Information (“ESI”) may be stored. ESI may be maintained in multiple locations, including employees’ assigned network drives, shared drives, email archives, back up files,[2] the hard drives of employees’ home and work desktop and laptop computers, and employees’ cell phones, CDs, DVDs, PDAs, and flash drives, among other locations.[3] Through communication with their clients, legal counsel should first identify each location they may have stored relevant electronic documents. Legal counsel should also educate themselves on their clients’ document retention policies and consider whether the policies allowed for potentially relevant documents to already be discarded, advise their clients on any modifications they should make to these policies (or on how to create such policies if they do not already exist), and advise them on how to implement and enforce a litigation document hold (i.e., the preservation of documents potentially relevant to the litigation). Finally, at this initial stage of the process, legal counsel should speak with clients’ Information Technology (IT) staff to learn about the clients’ computer systems, including what software programs they use and whether any specific document collection challenges may exist.

Armed with a good understanding of a client’s electronic data, legal counsel should be ready to discuss e-discovery issues with opposing counsel. Prior to initiating any document searches or collections, counsel ideally would have discussed with opposing counsel the custodians from whom documents will be collected, the search terms used to collect the relevant responsive data, and the format in which the e-discovery will be produced (e.g., TIFFs[4], PDFs,[5] or native files[6] and with or without metadata[7]). The parties are well-advised to discuss the details of the quality control measures that will be taken to ensure that the selected search terms are not producing too much irrelevant data or failing to produce relevant documents (e.g. the percentage of the data set that should be tested with the search terms), along with the costs associated with these tests. Quality control tests at the initial stages of the collection process can be a helpful part of the e-discovery process because, without them, parties may risk having to completely redo expensive searches or face criticism for producing

too much or too little relevant data. Ideally, the parties would reach written agreement on key aspects of the client's e-discovery plan, including division of costs among the parties, but at the very least, legal counsel's search plans should be transparent to opposing counsel and memorialized in writing. To the extent an agreement cannot be reached on one or more of these issues, counsel should consider seeking guidance from the court prior to engaging in expensive discovery that could ultimately be subject to motion practice.

Communication and transparency with one's opponents is not only advisable at the beginning of the discovery process but should be addressed throughout the process. It is almost inevitable that in today's e-discovery landscape unexpected issues will arise during the course of a document collection. For example, a quality control check may reveal that the search terms the parties originally agreed upon are producing a large number of irrelevant documents, or false positives. It may be in both parties' best interest to try to agree on a more narrow set of search terms or a fee sharing arrangement if opposing counsel still wants to include search terms that appear likely to produce a great number of false positives and/or are unlikely to produce relevant data. Alternatively, a quality control check may reveal that the search terms may be missing relevant documents, and therefore, the parties can work together to revise the search terms during the initial stages of the collection process, avoiding a potentially expensive and time-consuming "redo" later.

Counsel ideally should communicate with computer specialists to ensure that ESI is being collected in the most cost efficient and timely manner, while also minimizing the chance of responsive documents being missed. "The litigation support professional...is the gatekeeper to the electronic data acquired and produced in litigation matters." [8] Computer specialists are oftentimes needed to (1) conduct extensive key word searches throughout multiple databases and files containing millions of documents; (2) de-duplicate the results of these searches so attorneys do not have to review the same documents more than once; (3) run quality control tests on the search terms; (4) convert native files to TIFF files so portions of the documents can be redacted prior to production or so the production of metadata can be avoided; [9] and (5) collect and preserve residual data [10] and metadata, [11] which can be key information in litigation disputes. Even a small misunderstanding on any of these issues can have far-reaching consequences. As one commentator has said, "The failure to define even the simplest terms (such as 'preservation') may lead to failures in the overall process. In addition to clearly defining terms, IT and legal must work together to ensure that data management protocol is repeatable and defensible." [12] This level of communication between attorneys and computer specialists will yield benefits in today's litigation landscape--especially when the failure to preserve, locate and/or produce relevant documents can result in significant sanctions to the producing party and delay of a case.

There Should Also Be Effective Communication During the E-Discovery Review Process.

Communication is also important to help ensure consistency in the document review process. Today's review process in some complex cases may involve millions of pages of discoverable material^[13] and require teams of reviewers. These reviewers face numerous decisions throughout the review process, and ensuring consistency among review decisions is a challenge. Consider, for example, email messages that are sent to numerous individuals and groups at one time either directly or through "cc" or "bcc", all of whom may reply to some or all of the email recipients or forward these messages to other individuals or groups. This process can be repeated numerous times, creating a multiplicative effect.^[14] As a result, each of the messages within the email chain or sub-chains may show up in multiple electronic storage locations, and thus, may be reviewed more than once by the same or different reviewers. Basic de-duplication cannot eliminate this challenge because the emails are considered different to the extent that there is a new reply on the chains or if they are forwarded to different individuals. This means that the same email messages may be reviewed on multiple occasions for (1) relevancy, (2) responsiveness to the opponent's discovery requests, and (3) privilege. With so many subjective judgment calls to be made on almost unmanageable numbers of documents by multiple reviewers over an extended period of time, along with human error, the chance of production inconsistencies is high, if not inevitable. Moreover, these inconsistencies are readily discoverable by opposing counsel using an electronic search. For example, if opposing counsel reviews one email chain where a certain message is redacted and another chain in which the same message is not redacted or sees that a particular document has been disclosed in its entirety but then also sees the same document's description in the privilege log, there is a good chance that opposing counsel will complain to the court that the production is unreliable. Even litigants who use their very best efforts may inevitably face the revelation of such inconsistencies. As a result, a court may order the producing party to redo the expensive and time-consuming review process or even issue sanctions, as discussed in more detail below.

To minimize these inconsistencies in the review process, co-counsel ideally should discuss review guidelines at the onset of the process and continue to communicate as production issues and questions arise during the course of the review. Furthermore, there should be communication with the computer specialists about the technical steps they are taking to ensure consistency in production decisions. For example, certain software programs or quality control measures might help minimize inconsistencies and identify errors in the production decisions. Finally, reaching an agreement with opposing counsel prior to production that any privileged documents inadvertently produced will be returned to the producing party and will not constitute a waiver of the privilege (i.e., a "clawback" agreement)^[15] will help mitigate errors when they happen and ensure consistency in production (e.g., it will be harder for opposing counsel to say that the inadvertent production of one document means that all documents related to that subject matter should have been produced but were not).

Communication is Advisable to Minimize the Risk of Discovery Sanctions.

Although some judges may still be in “catch up” mode as they continue to learn about the intricacies of electronic document preservation and collection, judges in general are becoming more attentive to and sophisticated about e-discovery issues.[16] As their knowledge grows, their expectations with respect to companies’ preservation efforts (e.g., ideally having a document retention policy in place, issuing litigation holds to potential custodians, addressing the metadata issues, etc.) and expectations with respect to the sophistication of a companies’ document searches will continue to grow[17]—and these preservation and collection efforts are commonly judged in hindsight. E-discovery disputes and the threat of sanctions are being used by litigants with increasing frequency when it is in their interest to do so, and courts are not holding back on issuing sanctions related to e-discovery preservation and production failures. For example, in *USA v. Phillip Morris USA Inc.*,[18] the court ordered Phillip Morris to pay \$2.75 million in sanctions for destroying relevant emails and further ordered that 11 of its potential witnesses, including at least one key witness, could not testify at trial because they did not comply with the document retention policies. In *In re Prudential Sales Practices Litigation*, the court ordered that Prudential pay a \$1 million sanction due to management’s “haphazard and uncoordinated” policy of informing employees about their duty to preserve electronic documents.[19] In *In re Seroquel Products Liability Litigation*, the court ordered sanctions (while reserving ruling on the type or amount of sanctions) for the defendant’s failure to produce relevant electronic documents.[20] Strikingly, the court concluded that the defendant’s key word search for relevant documents, which included 60 search terms, 80 custodians, and the production of 10 million pages, was inadequate.[21] In *Pension Committee of the Univ. of Montreal Pension Plan v. Banc of America Securities, LLC*, the court found that thirteen plaintiffs had committed discovery violations, including failing to timely issue a written litigation hold, preserve all relevant evidence, request documents from key custodians, supervise custodians’ collection efforts, and submit accurate declarations regarding the document collection efforts.[22] As a result of these findings, the court sanctioned the plaintiffs by finding that the jurors should be instructed that the plaintiffs failed to preserve evidence and that the jurors may presume that such lost evidence was relevant and would have been favorable to the defendants.[23] The court further ordered that plaintiffs pay defendants their reasonable costs, including attorney fees, related to the sanctions motion and sanctions discovery.[24]

The issuance of sanctions based on the insufficiency of a key word search is especially disconcerting in light of the fact that key word searches are the primary tool for locating potentially responsive documents within the thousands, and oftentimes millions, of pages of a company’s ESI. Keyword searches are imperfect—they do not catch everything. The risks of overlooking relevant documents can never be eliminated—only minimized by reasonable steps that may include, when appropriate, hiring experienced litigators and litigation support professionals who know how to run extensive and advanced key word searches in multiple databases and run quality tests to check keyword search results for completeness. “[W]hile key word searching is a recognized method to winnow relevant

documents from large repositories, use of this technique must be a cooperative and informed process. . . .Common sense dictates that sampling and other quality assurance techniques must be employed to meet requirements of completeness.”[25]

Education That Email Messages Carry Significant Litigation and Reputational Risks Is Important.

Education as to the risks of electronic communication is important today. The increasing reliance on email and the growing sophistication of electronic discovery increases the likelihood that evidence damaging to one’s case may be created and uncovered. People tend to bare their souls in emails more so than in letters or paper memoranda of times gone by. “Emails can be particularly important and culpable evidence because of people’s tendency to communicate informally and reveal facts they never would memorialize in writing on a piece of paper containing their signature.”[26] In this sense, litigation has changed – a case may be won or lost depending on which party has the most revealing or undesirable email messages. Even if emails do not contain damaging evidence, they may contain comments that would be extremely embarrassing to a to a client or witness if randomly picked up by a search term and inadvertently disclosed, such as inappropriate jokes or derogatory comments.

As a result of these growing trends, companies should educate their employees as to (1) the risks associated with sending or receiving potentially embarrassing emails or reviewing inappropriate material while at work and (2) the steps that they should take to avoid the creation of adverse evidence. “Companies that take charge by proactively managing enterprise information reduce litigation risks, maintain compliance more efficiently, and save a bundle in the process.”[27] Your opponent in litigation may well have “cleaner” email due to an education program and, as a result, have an advantage in the litigation. Human nature cannot be changed, but education may reduce, although it cannot eliminate, risk.

Communication With Opposing Counsel May Help Ensure that Evidence Helpful to One’s Case Will Be Discovered.

Gone are the days in which legal counsel can request particular types of documents from their opponents and be assured that what they receive in response to their requests, even from opponents acting in good faith, includes all potentially relevant and helpful ESI. As the field of electronic data continues to grow dramatically and e-discovery tools become more sophisticated, the risk of missing key evidence helpful to one’s case continues to increase. Discovery requests in today’s world must specifically describe the types of computer data that should be included in a discovery production, including back up files, residual files, and metadata, if potentially helpful. Moreover, the requesting party must have a full understanding of the nature and extent of the electronic search conducted by its opponent in response to the discovery requests. A requesting party cannot simply assume that its opponent is technologically savvy and knows where to look for ESI.

Conclusion

Litigants should be proactive in minimizing the risks and expenses of electronic discovery by encouraging communication at all levels. Additionally, education programs that explain to corporate employees and remind them of the risks associated with sending personal emails and utilizing social websites while at work are important. Taking these steps may result in additional up front expenses, but will yield benefits when and if litigation arises.

[1] Lange, Michele, et al., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, (2009), at 2.

[2] "Backup data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster." www.renewdata.com/e-discovery-glossary.php

[3] See Perkins, Kathy, et al. "Byte Me! Protecting Your Backside in an Electronic Discovery World (Not Just for Litigators)", 76 J. Kan B.A. 22, 23 (2007).

[4] TIFF stands for Tagged Image File Format. TIFF is "one of the most widely supported file formats for storing bit-mapped images." Files in TIFF format often end with a .tif extension. The Sedona Conference Glossary (May 2005).

[5] PDF stands for Portable Document Format. A PDF is an imaging file format technology developed by Adobe Systems. PDF captures formatting information from a variety of applications in such a way that they can be viewed and printed as they were intended in their original application by practically any computer, on multiple platforms, regardless of the specific application in which the original was created. PDF files may be text-searchable or image-only. The Sedona Conference Glossary (May 2005).

[6] A native file is a file saved in the format of the original application used to create the file. The Sedona Conference Glossary (May 2005).

[7] "Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted." The Sedona Conference Glossary (May 2005).

[8] Levy, Douglas, "With E-Discovery Becoming the Norm, Demand for Legal Support on the Rise," *Michigan Lawyers Weekly*, September 1, 2008.

[9] Kelly, Robert E., "Understanding Electronically Stored Information," *Business Law Today*, September/October 2007 ("By producing documents as TIFF files, you can avoid producing metadata . . . It allows you to . . . redact privileged materials . . .").

[10] Residual Data “refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted, in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.” The Sedona Conference Glossary (May 2005).

[11] “Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed.” The Sedona Conference Glossary (May 2005).

[12] Jytyla, Regina A., et al., “ESI Management From Server Room to Board Room,” *LJN’s Legal Tech Newsletter*, March 2009.

[13] Dolan, Mike, et al., “The Tipping Point,” *Legal Management*, August 2009.

[14] Perkins, Kathy, et al. “Byte Me! Protecting Your Backside in an Electronic Discovery World (Not Just for Litigators)”, 76 J. Kan B.A. 22, 31 (2007).

[15] See Federal Rule of Evidence 502.

[16] Jytyla, Regina, et al., “ESI Management From Server Room to Board Room,” *LJN’s Legal Tech Newsletter*, March 2009.

[17] Jytyla, Regina A., et al., “ESI Management From Server Room to Board Room,” *LJN’s Legal Tech Newsletter*, March 2009 (“[R]ecent case law reveals that courts are holding corporations to stricter compliance standards in the development of repeatable and defensible data management and e-discovery protocol”).

[18] 327 F.Supp.2d 21, 25-26 (D.D.C. July 21, 2004).

[19] 169 F.R.D., 598, 615, 617 (D.N.J. 1997).

[20] 244 F.R.D. 650, 661, 665 (M.D. Fla. 2007).

[21] *Id.* at 661-62.

[22] 2010 WL 184312, at *10, 12 (S.D.N.Y. January 15, 2010).

[23] *Id.* at *23.

[24] *Id.* at *24.

[25] *Id.* at 662.

[26] Lange, Michele, et al., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, (2009), at 2

[27] Talley, Ursula, “Proactive E-Discovery Can Reduce the Risks of Lawsuits,” *Andrews Automotive Litigation Reporter*, September 16, 2008.

This publication has been prepared for the general information of clients and friends of the firm. It is not intended to provide legal advice with respect to any specific matter. Under rules applicable to the professional conduct of attorneys in various jurisdictions, it may be considered advertising material. The advice contained in this article is not intended or written to be used, and cannot be used by a taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under law.

For more information visit our Web site at www.schiffhardin.com.

© 2010 Schiff Hardin LLP