Effective E-Mail Discovery

Be Proactive and Combine Practical,Technical and Legal Strategies

By Jon M. Talotta

As we all know, e-mail is often the key source of evidence in litigation. E-mail is probably the most common form of written communication in the workplace and at home. More importantly, an e-mail may form a contract, contain statements concerning important facts, knowledge or intent and, in some instances, be actionable in and of itself (e.g., defamation, phishing). In addition, although they are creating a writing that can be easily forwarded and potentially lasts forever, people are remarkably unguarded in their use of e-mail as compared to other written communication. Thus, e-mail is usually the most revealing (and often the only) contemporaneous record of a party's thoughts and intentions as events or transactions unfold. As we also know, discovery is driven by two fundamental goals: protect your client's information; and obtain information from others that you may need for your case. E-mail discovery, however, can be very expensive for both the requesting party and the producing party, and producing e-mail always involves the risk of inadvertently disclosing privileged information, particularly in large productions. As a result, lawyers must be proactive from the outset, combining practical, technical and legal strategies in order to protect client information and maximize the return on a client's investment in e-mail discovery. To a large extent, the keys to effective e-mail discovery apply generally to electronically stored information (ESI) in all aspects of electronic discovery (e-discovery). This article focuses on e-mail in order to frame the discussion in a context likely to be familiar to all readers.

Client E-Mail: From the Outset, Preserve and Investigate

In terms of protecting your client's e-mail and other information, you cannot "hide the ball," but you can preserve and investigate your client's records and systems to safeguard against spoliation and manage costs.

Preservation. Upon notice of impending litigation, take steps to preserve your client's potentially relevant e-mail. Your client may already have an ESI policy in place covering e-mail and litigation "hold" procedures. If so, get a copy, determine whether it has been followed in the past, and ensure that any litigation hold procedures are followed going forward. If not, establish litigation hold procedures as soon as practicable. Sanctions for spoliation can be severe.

Investigation. At the same time, meet with your client's information technology (IT) personnel, whether your client's information system is a single computer or a multi-server infrastructure. Meeting with management is not enough, but it can be helpful to give both IT personnel and management a written questionnaire to complete before your meetings.[1] The responses will help you ask informed questions and can be useful later.

Technical issues. In order to plan an effective e-mail discovery strategy, you have to consider more than the issues likely to be relevant in the litigation—you must understand the basics of how your client's e-mail is managed (e.g., system structure, storage and disaster recovery procedures). If you do not educate yourself, it will be difficult to establish an efficient litigation hold (which can be unduly burdensome if too broad and dangerous if too narrow). Moreover, you will not understand whether certain e-mail is inaccessible or overly expensive to collect and, as a result, miss opportunities to discuss these issues with opposing counsel early in the case. In addition, you may not be able to assess whether use of an e-discovery vendor would be helpful or necessary.

Opposing Party E-Mail: Broad Requests May Be Counter-Productive

Conducting e-mail discovery on an opposing party involves choices. Broad requests are likely to cover the available information you need, but can result in massive productions that are costly to review. As a result, attempt to gather information about an opposing party's e-mail and systems early on, in order to make informed decisions about the nature and scope of your discovery requests.

Preservation. Consider sending a litigation hold letter to the opposing party to provide clear notice of preservation obligations. This will set up a framework for resolving disputes over incomplete productions or spoliation that may arise later.

Investigation. Courts now expect, if not require, counsel to cooperate on e-discovery issues.[2]

Pre-discovery conferences are an opportunity to explore preservation, scope, accessibility and cost issues prior to discovery. If your client wants to limit the scope of e-mail discovery, you may want to explore whether the opposing party will produce or accept production of e-mail limited to specific individuals or agreed-upon topics or search terms.[3] In addition, if an opposing party has lots of e-mail or complex systems, you may want to depose its IT personnel and/or serve targeted interrogatories prior to serving the bulk of your merits discovery requests.

Technical issues. Here, as well, understanding technical issues relating to the opposing party's e-mail and systems may eliminate there flexive urge to serve broad requests that are easy to draft but can result in massive productions.[4] More importantly, you will be in a better position to anticipate potential objections to your discovery requests, including whether an opposing party may assert that certain e-mail is inaccessible or too expensive to collect, and thereby reduce the chance that the opposing party will be able to shift some of its costs onto your client.

Third Party E-Mail: Can Be Very Helpful to Your Case

Do not overlook. There usually is little downside to serving requests on third party individuals or entities, and the return on your investment can be significant. Of course, a third party may have relevant e-mail or other information that neither your client nor an opposing party has in its possession. A less obvious reason for requesting third party e-mail is to obtain metadata from e-mail sent by the third party that would not be available in your client's or another party's copy, such as the blind copy (bcc) recipients of an e-mail.

Usually not difficult to obtain. Assuming the third party resides in the United States, it is relatively easy to request e-mail or related information in federal or state court proceedings. In some instances, your client may not be able to identify the third party, because the discovery is triggered by an e-mail received from an anonymous e-mail address. For example, a defamatory e-mail sent to your client and others from an anonymous e-mail address is not very useful until the true identity of the author is known. This type of third party dis-

See **E-MAIL** *page 11*

covery is often directed at Internet service providers (ISPs).[5] Once you have determined a third party may have relevant e-mail, you should consider sending a litigation hold letter, particularly if it is unlikely that the third party, such as an ISP, is aware that it may be subject to discovery in your dispute.

Preparing Client E-Mail Productions: Combine Practical, Technical and Legal Strategies

The process of producing e-mails (as with all documents) can be broken down into four phases: identification; collection; final review; and production.

Identification. The initial investigation of your client's information systems will help you identify the sources of potentially responsive e-mail more quickly. Identify all sources, including live files, archives and disaster recovery files, whether on internal or out-sourced systems or servers, computers, laptops, or mobile devices. Do not forget about employee home computers.

Collection. You do not have to collect all potentially responsive e-mail, but you need to identify it and be able to articulate a reasonable justification for what is not collected based on inaccessibility and/or cost.[6] In other words, as the "marginal utility" of collecting certain e-mail decreases, your client may be able to forego collecting the e-mail or shift the cost of collection onto the requesting party.[7] Document management software can be used to eliminate some non-responsive e-mail and identify duplicates prior to the final review to save costs. In addition, you need to ensure that your client's IT personnel remain informed throughout this process, because they may have to provide affidavits or testimony later, to authenticate and/or establish a foundation for e-mail you are attempting to introduce into evidence. Do not assume that your client's e-mail or other ESI will simply fly into evidence. Your records custodian should be well-versed in the maintenance and storage of your client's ESI.[8]

Final review. The most critical—and expensive—aspect of an e-mail production is usually the final review for responsiveness and privilege. It is difficult to completely automate this process, but search technology usually can identify a large percentage of potentially privileged e-mail. There always is a risk that privileged information will be inadvertently produced, particularly in very large productions. Because the rules on waiver of privilege vary across jurisdictions,[9] it is worth attempting to work out "quick peek" or "claw back" arrangements with the requesting party, to avoid waiver and reduce review costs.[10] Agreements to forego the preparation of privilege logs, or at least limit what must be logged (e.g., documents relating to key people or issues), can reduce costs as well. Finally, e-discovery vendors can be a valuable asset at this stage, but you too must stay on top of the technical details.[11]

Production. E-mail can be produced in a variety of formats: native files (e.g., PST); exported files (e.g., for use with database software); images (e.g., TIFF, PDF); and hard copy. The amount of information included with each e-mail (e.g., metadata, attachments), the level of searchability, and the ability to protect privileged information, vary with each format. For example, requesting parties often want native files, which contain metadata and attachments, rather than TIFF and PDF files, which might not. E-mail in native files, however, can be more difficult to Bates stamp and redact than in TIFF or PDF files. In the past, producing parties often attempted to limit the information provided in, and the searchability of, an e-mail production by producing the least functional format possible. Today, however, amended Rule 34(b)of the Federal Rules of Civil Procedure (effective December 1, 2006), gives the requesting party the ability to specify the format of the production. This change will no doubt influence the states to make changes as well. As a result, the safest approach is usually to produce e-mail in the same format that you intend to use during the litigation, unless you can articulate a reasonable basis for producing it in a different format.[12]

Reviewing and Managing Opposing/Third Party E-Mail Productions: Identify Potential Disputes Early, Stay Organized

Once you receive an e-mail production, you need to determine whether it is complete and, if not, whether e-mail is missing as a result of a disagreement over the scope of your requests, the routine deletion of e-mail, or spoliation. In addition, you need to organize and manage the e-mail production along with the rest of your case.

Production Disputes. Reviewing another party's e-mail production is almost expensive as the final review of your own productions (the former does not include privilege review). Your short-term objective is to assess the production's completeness as it relates to your discovery requests. Software usually is not enough.

Human review, depositions, and/or discovery responses often are necessary as well. Occasionally, disputes over completeness arise that may require a computer forensics expert to resolve. Forensic experts can inspect systems, devices and files, and may be able to recover deleted records or, in extreme cases, detect intentional spoliation.[13]

Document Management. Your long-term objective is to organize and integrate the e-mail production into the rest of your case. Here, in particular, document management technology and software can result in significant time and expense savings. This technology can enhance searchability and preserve annotations/notes and other related information in one centralized location, thereby reducing the duplication or repetition of your efforts.

Conclusion

This roadmap merely scratches the surface of e-mail discovery. There are many details and nuances underlying each of the issues discussed above. The precise path to effective e-mail discovery (as with all discovery, ESI-related or otherwise) will depend on the circumstances of each case, including the information systems of your client and the other parties involved. Nevertheless, if you are proactive from the outset, and can combine practical, technical and legal strategies, you will increase the likelihood of protecting your client's e-mail and other information, and of maximizing the return on your client's investment in e-mail discovery. ❐

Notes

1. An ESI questionnaire can cover: computer, server, and system structure and procedures; ESI storage and procedures; disaster recovery and business interruption procedures; and litigation hold procedures. ESI questionnaires can be tailored to address the specific issues relevant to a particular case. For example, in an employment case, the questionnaire might include questions about employee termination, departure, or transfer procedures.

2. For example, in federal court cases, counsel are required to address ESI-related discovery issues during the pre-discovery conference, pursuant to amended Rule 26(f) of the Federal Rules of Civil Procedure ("Federal Rule"), effective December 1, 2006.

3. *See, e.g.*, **J.C. Assocs. v. Fidelity & Guar. Ins. Co.**, 2006 U.S. Dist. LEXIS 32919 (D.D.C. May 25, 2006) (court approved collection of responsive documents based on search terms used to limit production of 1.4 million potentially responsive insurance claim files down to 454 files).

4. Similarly, if your client does not want, or cannot afford, to respond to broad requests, you may not want to serve them on an opposing party (i.e., you want to avoid having the well-known axiom "sauce for the goose is sauce for the gander" directed at your client as a result of your own requests).

See **E-MAIL** *page 12*

NORTH CAROLINA
BAR ASSOCIATION
SEEKING LIBERTY & JUSTICE

NORTH CAROLINA BAR CENTER
PO Box 3688
Cary, NC 27519-3688

Nonprofit Organization
U.S. Postage
PAID
Raleigh, NC
Permit Number 297

E-mail *from page 11*

5. Virginia and many other jurisdictions have statutory and/or common law rules that permit so-called "John Doe" discovery. *See, e.g.,* Va. Code Ann. § 8.01-407.1 (providing for discovery of identity of "persons communicating anonymously over the Internet"); **America Online, Inc. v. Nam Tai Electronics, Inc.,** 264 Va. 583 (2002) (permitting "John Doe" discovery in Commonwealth).

6. For example, amended Federal Rule 26(b)(2)(B), effective December 1, 2006, requires a party to identify in its discovery responses ESI that exists but is deemed "inaccessible" due to the infeasibility or cost of collection. The rule sets up a framework for a producing party to object to an e-discovery request and thereby seek to shift the costs onto the requesting party if the collection is actually performed.

7. A leading common law analysis on cost-shifting is set forth in Judge Scheindlin's series of opinions in the now-famous Zubulake case. *See, e.g.,* **Zubulake v. UBS Warburg LLC,** 217 F.R.D. 309 (S.D.N.Y. 2003).

8. *See, e.g.,* **In re Vinhnee,** 336 B.R. 437 (B.A.P. 9th Cir. 2005) (affirming bankruptcy court exclusion of electronic records submitted by American Express to establish creditor status in debtor's proceeding, because American Express' custodian of records lacked sufficient knowledge of the company's ESI management and storage procedures).

9. The ABA has proposed new Federal Rule of Evidence 502, which is intended to promote uniformity across jurisdictions with respect to the rules on waiver of privilege. Among the provisions, subject matter waiver is limited to "unusual" situations; inadvertent disclosures do not result in waiver if reasonable steps were taken prior to and after the disclosure; intentional disclosure of privileged information to the government during an investigation will not result in a waiver as to third parties; and federal court orders regarding waiver will be enforceable against non-parties in other federal and state proceedings.

10. These arrangements allow the requesting party to conduct an initial ("quick peek") review of the collected e-mail and to request selected e-mails to be produced. The producing party then conducts a privilege review of just the selected e-mail and retains any privileged e-mail ("claw back") prior to the actual production. See Fed. R. Civ. P. 26(f)(3) (as amended, effective December 1, 2006).

11. Recent headlines confirm the need to remain informed on technical issues. In connection with the ongoing Enron litigations, an e-discovery vendor prepared productions that included numerous e-mail containing no text. At first, it was suspected that the e-mail might have been erased, but ultimately was determined that no e-mail had been erased and that the problem was software-related. See Software Glitch May Have Erased E-Mail Text in Enron Suits (August 10, 2006) (available at *http://biz.yahoo.com/law/060810/fc7314b1eaf35588924f84e05fcc9b81.html?.v=1*). Nonetheless, the story is a cautionary tale – even your e-discovery expert can have technical problems.

12. *See, e.g.,* **CP Solutions PTE, Ltd. v. General Electric Co.,** 2006 U.S. Dist. LEXIS 27053 (D. Conn. Feb. 6, 2006) (producing party ordered to produce native files with attachments included; TIFF files without attachments not reasonable); **Williams v. Sprint/United Mgmt. Co.,** 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005) (producing party ordered to produce metadata previously "scrubbed" from Excel spreadsheets in production, because metadata was relevant to issues in litigation).

13. Sanctions for spoliation can include default judgments. *See, e.g.,* **Krumwiede v. Brighton Assoc. LLC,** 2006 WL 1308629 (N.D. Ill. May 8, 2006) (default judgment entered for willful deletion of files). Significant sanctions have been imposed in several prominent cases over the past two years for discovery abuses relating to e-mail. *See, e.g.,* **Zubulake v. UBS Warburg LLC,** 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (adverse jury instruction against defendant and costs imposed for willful destruction of e-mail); **Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.,** 2005 WL 679071 (Fl. Cir. Ct. March 1, 2005) (adverse jury instruction against defendant for willful destruction of e-mail; counsel disqualified; burden shifted to defendant to prove it did not commit fraud).

TALOTTA IS A SENIOR LITIGATION ASSOCIATE IN HOGAN & HARTSON LLP'S NORTHERN VIRGINIA OFFICE. HE IS A GRADUATE OF THE UNIVERSITY OF VIRGINIA SCHOOL OF LAW, SERVED AS A LAW CLERK TO THE HONORABLE JAMES C. CACHERIS (E.D.VA.) AFTER LAW SCHOOL, AND FOCUSES HIS LAW PRACTICE ON COMPLEX LITIGATION AND COUNSELING CLIENTS ON A RANGE OF COMMERCIAL MATTERS, INCLUDING INTELLECTUAL PROPERTY, THE INTERNET, AND INSURANCE COVERAGE.

Editor's Note: Article originally appeared in The Virginia Bar Association News Journal. *Reprinted with permission.*