By David H. Schultz and J. Robert Keena

Navigating the Perils of Discovery in the Electronic Information Age

On the day they are admitted to practice law, lawyers swear under oath to provide zealous advocacy to all clients. In Michigan, Rule of Professional Conduct 1.1 requires that "A lawyer shall provide competent representation to a client. A lawyer shall not: (a) handle a legal matter which the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it." Attorneys today are faced with an overwhelming array of new challenges created by the proliferation of information stored in an electronic format. From pre-discovery stages of a lawsuit through trial, true zealous advocacy requires a solid understanding of electronic discovery issues.

Electronic files and e-mail are, by their very nature, fragile. While electronic files are easy and convenient to create and duplicate, they are also easy to alter or destroy. Accordingly, one of the foremost issues in electronic discovery is preservation.[1] Preservation letters should be sent to all parties and non-parties in possession of potentially relevant data. In some cases the additional step of securing a preservation order may be required. As the case moves forward, monitoring preservation compliance can be important and potentially quite fruitful.

Once the perils of preservation have been navigated, attorneys must address the disclosures required by FR Civ P 26. The disclosure of "data compilations," such as electronic files, databases, and e-mails, following a full investigation of the case is required by Rule 26(a)(1)(B). This means, at a minimum, determining all sources and locations of electronic data.[2] Data will commonly be located on individual desktops and laptops, network hard discs, removable media such as floppy discs, tapes, and CDs, and personal digital assistants, such as Palm Pilots. Data may also be in the possession of third parties, such as Internet service providers and on the computer systems of other peripherally involved entities. Determining the volume of e-mail and other electronic information is crucial but can be difficult to do without the assistance of an experienced electronic discovery expert.

FR Civ P 26(a)(2) calls for the disclosure of any person who may be used at trial to present evidence under FRE 702, 703, or 705. Counsel must determine whether to disclose any electronic discovery experts involved in the case under this rule. Though electronic discovery experts possess the kind of "scientific, technical, or other specialized knowledge" contemplated by FRE 702, a parallel can be drawn between such an expert and a records custodian who simply retrieves, photocopies, and certifies hard copy documents. The safest approach may be to err on the side of over-disclosure by including such electronic discovery experts in the Rule 26(a)(2) disclosures.

In cases that require expert computer forensic work, an additional expert should be retained. This expert should be provided with only the information necessary to formulate and present opinions on the evidence and should not perform any hands-on processing of electronic information. In some cases, the court will even retain its own expert to serve as an officer of the court to deal with the electronic information.[3]

One of the most useful electronic discovery management tools may be the FR Civ P 16 pretrial conference. As with a Rule 26(f) meeting, counsel must be prepared with the salient facts regarding all electronic data involved in the case. Doing so will assist in limiting the scope of discovery required from one's client while maximizing the disclosures from opposing parties. In many situations it may be necessary to provide the court with expert testimony on the nature, location, and volume of electronic data, as well as the time and cost involved in producing it.

Topics for discussion at the Rule 16 conference may include preservation of evidence (including whether backup, archival, and "deleted" files will be exchanged[4]), preliminary disclosures of the parties' computer systems (including numbers, types, and locations of computers, operating systems in use, and backup schedules), document processing and production formats,[5] testifying experts, and anticipated evidentiary disputes.

If, for jurisdictional reasons or otherwise, a Rule 26 initial disclosure related to "data compilations" has not occurred, practitioners may acquire the data through a combination of interrogatories, requests for documents, and depositions. A request for "all electronic data" will likely result in an objection based on burden or expense, and courts have been inconsistent on how deeply they will allow a discovering party to dig.[6] As such, discovery requests must be specific and exhibit an understanding of how electronic data is created, stored, and destroyed.

Electronic evidence also creates new and unique ways for your client to cause spoliation of evidence. When copying data for production or review, failure to make sector-by-sector images before viewing may result in spoliation.[7] Simply booting up a computer can destroy "slack" and "temporary" files. Clicking on a file rather than properly copying it can

change its last access date and lead to sometimes-harsh sanctions or inadmissibility.

Because of this, no party should avoid bringing a motion to compel to enforce the production of this data knowing that if the data is produced in an altered state, spoliation may have occurred. Just as certain, because of the inconsistency in the case law, no attorney should pass on the opportunity to seek a protective order to prevent the destruction of this data. Sanctions for spoliation of evidence include adverse inferences or presumptions, preclusion of evidence, monetary sanctions, and dismissal or default.

Once the minefield of electronic discovery has been traversed, spoliation has been avoided, and no "smoking gun" e-mail has been discovered forcing settlement or supporting summary judgment, the issue of the admissibility and use of electronic evidence at trial remains. To be admissible, e-mail and other electronic evidence must be authenticated according to FRE 901(a), and the evidence must clear any hearsay hurdles. Computer records may be admitted under the business records exception to the hearsay rule.[8]

As technological developments simplify our daily activities, they simultaneously create trails of data complicating legal discovery. The question a litigator should ask at each stage in the process—from investigation through trial—is whether one can provide zealous advocacy without engaging in electronic discovery. With 70 percent of all data now stored in electronic form,[9] the responsible practitioner knows the answer. ✦

David H. Schultz is associate legal counsel and electronic discovery consultant for Ontrack Data International, Inc. (www.ontrack.com/datatrail), a company specializing in electronic discovery and computer forensics.

J. Robert Keena (jkeena@hjlawfirm.com) is an attorney with Hellmuth & Johnson PLLC in Minneapolis, MN. His practice includes litigation involving electronic discovery and consulting on document retention.

FOOTNOTES

1. *Linnen v A H Robins Co,* 1999 WL 462015 (Mass Super June 16, 1999).
2. *Kleiner v Burns,* 2000 WL 1909470 (D Kan Dec. 15, 2000).
3. *Simon Property Group v mySimon, Inc,* 194 FRD 639 (SD Ind 2000).
4. *Superior Consultant Co v Bailey,* 2000 WL 1279161 (ED Mich Aug. 22, 2000) (ordering defendant to create and produce for plaintiff a backup file of defendant's laptop computer).
5. *In re Air Crash Disaster at Detroit Metro,* 130 FRD 634 (ED Mich 1989) (ordering the aircraft manufacturer to provide relevant data on computer-readable tape even though the data was already provided in hard copy).
6. *Demelash v Ross Stores, Inc,* 20 P3d 447 (Wash Ct App 2001).
7. *Gates Rubber Co v Bando Chem Ind,* 167 FRD 90 (D Colo 1996).
8. *State of Wash v Ben-Neth,* 663 P2d 156 (Wash Ct App 1983).
9. Lori Enos, E-Commerce Times, *Digital Data Changing Legal Landscape,* May 16, 2000 http://www.ecommercetimes.com/perl/story/3339.html.