The Impact of Tech
Finding and Obtaining

NOLOGY: EVIDENCE

The proliferation of electronic data has made the process of gathering information for litigation much more expensive, complicated, and time consuming.

by Bill Ramsey and Phillip Hampton

Technology has had a significant impact on the practice of law. It has touched almost every aspect—word processing, time and billing, electronic research, communications by voice and e-mail, the presentation of information in court, and so forth. Perhaps technology's greatest impact has been on discovering and obtaining information in litigation.

Prior to the proliferation of electronic information and data, the discovery of information was relatively simple and straightforward, even in large cases. Discovery in civil and criminal cases consisted primarily of taking statements of witnesses and parties by deposition or otherwise and gathering hard copies of documents. Generally, the parties would first gather all relevant documents and then question the witnesses about those documents. Technology has changed the process dramatically.

At first, many legal pundits argued that the existence of electronic information would make the discovery process much easier and more thorough. These pundits predicted that a lawyer would be able to "push a button" and gather all relevant electronic information. Then he could push another button that would sort the information and place it in the appropriate categories. Finally, with the push of one more button, all of the information could be recalled instantaneously. Unfortunately, these pundits were incorrect. The proliferation of electronic data has made the process of gathering information for litigation much more expensive, complicated, and time consuming.

Electronic Information Is Voluminous and Complicated

Recent studies indicate that 90 percent of all documents created since 1999 are in digital format. In the past 300 years, mankind created 12 exabytes of electronic information. (One exabyte equals a billion gigabytes. The total of all words ever spoken by humans is approximately five exabytes.) The amount of electronic information is estimated to double in the next two years. It is estimated that 10 billion e-mails are sent worldwide each day.

In addition, the sources of electronic information are endless. There are computer hard drives, backup tapes, floppy disks, network file systems, CD-ROMs, personal information managers, personal digital assistants, laptops, e-mail, electronic machines used with manufacturing, cell phone information, electronic information stored in the computer systems of automobiles, and so on. Moreover, electronic information proliferates rapidly. A single e-mail with an attached word processing document can easily be copied 20 or 30 times within a very few minutes through the process of creating the document, e-mailing it to others, who forward it to others, and so on. Many times the information, especially e-mail, is very informal and sent without a lot of thought. Electronic files are also difficult to destroy. "Deleting" a file does not always erase the data from the hard drive. Data can be automatically saved without the user's knowledge. Even files that have been properly destroyed may be recovered from backup media.

Electronic data can also contain "metadata." For example, in a word processing document, the metadata will consist of the author, the computer it was created on, the date it was created, the number of times it has been revised, the people who have reviewed and revised it, and so on. For e-mail metadata there

continued on page 10

continued from page 9

is an industry standard called RFC822. That standard requires that all e-mail header labels contain up to 24 different pieces of information. Those headers are not usually seen by the persons who create and receive e-mail messages, but they are there nevertheless.

Valuable electronic information can easily be lost inadvertently. Electronic information can be electronically forged with relative ease. Electronic information contained in outdated or "legacy" systems may be very difficult and expensive to obtain. With all these issues in mind, we will discuss the practical and legal considerations encountered when obtaining or producing electronic discovery in litigation.

In civil litigation, there are specific rules of procedure that govern how information is to be obtained. The rules are equally applicable to paper and electronic information.

Planning for Electronic Discovery

In planning for electronic discovery, a lawyer must first decide whether the discovery is to be taken from, or on behalf of, a governmental entity. There are special issues for governmental entities. For example, in Tennessee there is the Open Records Act, T.C.A. § 10-7-503. This statute basically provides that most information gathered by governmental agencies in Tennessee is open to public access and can be obtained upon request by any citizen. The case that is most constructive on this issue is *The* Tennessean *v. Electric Power Board of Nashville*, 1997 Tenn. App. LEXIS 411. In that case, the Tennessee Supreme Court ruled that a governmental agency—here, NES—had to provide its customer names, addresses, and telephone numbers as a public record even though it did not maintain the information in its computer in the exact format in which it had been requested.

In addition, the State of Tennessee and most other governmental entities have electronic document retention policies that establish the electronic information that is saved and how it is saved. (See, for example, T.C.A. § 10-7-301).

There can be similar issues for nongovernmental entities that are producing electronic information. Often, large corporations have e-mail policies and electronic document retention policies that may be obtained prior to or during litigation. Having this information will make it easier to identify relevant electronic data.

In planning for either providing or obtaining electronic information, one should consider all of these matters.

Obtaining Electronic Information

In civil litigation, there are specific rules of procedure that govern how information is to be obtained. The rules are equally applicable to paper and electronic information. However, as might be expected, the proliferation of electronic information has raised new and interesting issues.

The rules that are applicable to electronic discovery are Fed. R. of Civ. P. 26(a) and 26(g) and Fed. R. Civ. P. 34. Those rules refer to "data compilations." The term "data compilations" is defined in the rules to cover virtually any type of electronic information. The State of Tennessee and most other states have similar rules of civil procedure. In Tennessee, they are Tenn. R. of Civ. P. 34 and Tenn. R. of Civ. P. 26.07.

Entities that anticipate having to provide electronic information should interview all information systems personnel and get an inventory of all electronic information. The entity should then establish a plan for the most efficient method of gathering, sorting, and separating the information into privileged and non-privileged categories and so on. The entity producing the information should be prepared to obtain estimates of the cost of retrieving and producing that information so that it can minimize the economic burden. It may be able to use the cost information and obtain a court order requiring the other side to pay the costs of producing it.

For parties seeking to obtain electronic information, it is often best to start with a "preservation of evidence" letter. This is a letter requesting the other party to maintain all electronic information that is relevant to the subject matter of the litigation and refrain from destroying it. This type of letter will often come in handy if you learn later that your adversary has actually destroyed relevant electronic information. The next step in obtaining electronic information is usually to send "interrogatories" to obtain information about the other party's computer systems. (Interrogatories are written questions that are to be answered under oath and in writing by your adversary.)

Finally, once you have sent out the interrogatories relating to electronic information, it is best to take the deposition of the person or persons in charge of your adversary's computer system. After obtaining all of that information, you can tailor electronic document requests (or requests for "data compilations") to the information you have obtained. If your adversary states that it just cannot produce this information from its computer systems, you can ask the court for something called "a request for inspection," in which you actually send your computer experts to your adversary's computer locations to take the electronic information directly from the computers themselves.

During the discovery process, issues may (and probably will) arise regarding electronic information that is not simply electronic "documents." As described above, there is "metadata," legacy data (computer information con-

tained on backup tapes of old systems), residual data, embedded data, replicant data, and so on. All of this data may be discoverable. All such information is potentially important and can sometimes be decisive in the litigation.

Electronic discovery can be very expensive and time consuming. In many cases there are arguments in litigation over who should actually be required to pay for the information. For example, many large corporations retain backup tapes. These backup tapes may number in the thousands. In order to restore that information, a party may be required to buy and set up an identical computer system, go through the process of restoring the data on the backup tapes, and then search through it. For large corporations, this process can become extremely expensive and time consuming.

In addition, issues may arise over whether or not the documents should be produced in both paper and digital form. If there are several electronic versions of the same information, there may be issues regarding how many of those are required to be produced. There may be disputes over whether or not the court's rules require disclosure of information that is not "a document"—such as metadata.

Parties who are not a part of the litigation may be required to produce electronic information. Discovery from such third parties is generally covered by Rule 45 of the Fed. R. of Civ. P. and Rule 45 of the Tenn. R. of Civ. P. The courts usually try to protect these third parties from undue burden and expense and to avoid compromising privacy and confidentiality of the third parties during the process.

There are also numerous evidentiary issues that may arise after obtaining the information, i.e., whether the information is admissible in court. For example, there may be an issue on whether the electronic information is authentic. See *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000). There may be issues regarding whether or not the electronic information is hearsay. See *Thomas v. Thomas*, 2001 W.L. 563306 (Ohio 2001); *Sea Land Service, Inc. v. Lozen International*, 285 F.3d 808 (9th Cir. 2002). There may be issues on whether the document is a business record and is an exception to the evidentiary rules regarding hearsay. *United States v. Russo*, 480 F.2d 1228 (6th Cir. 1973). There may be issues on whether or not evidence was purposefully or negligently destroyed. *Pennar Software Corp. v. Fortune 500 Systems, Ltd.*, 2001 U.S. Dist. LEXIS 18432 (N.D. Cal. 2001).

Although it is beyond the scope of this article, similar issues can arise in criminal cases. For example, how far must the government go to make sure it is providing exculpatory information as required by the Constitution? See *Brady v. Maryland*, 373 U.S. 83 (1963). These issues are interesting, and they are just emerging as issues in criminal law.

Obtaining Information Informally

Many times lawyers obtain information through processes other than formal discovery through the courts. The lawyers may hire private investigators or ask their clients to gather information for them. Care must be taken when gathering information informally. An honest mistake in judgment can result in significant problems.

For example, some clients, especially divorce clients, have the desire to place a tape recorder on a telephone. The telephone may be the home phone or a third person's. Generally, it is against the law, and indeed a felony under federal law, to record a telephone conversation (or a normal conversation for that matter) to which you are not a party. If you are a party to a conversation, you can record it. If the conversation (either a live conversation or telephone conversation) is recorded without authority from any of the participants, the evidence is generally not admissible in court, and recording it is a crime. Similarly, it is against the law to intercept or obtain e-mail messages without authority.

The statutes governing these issues are 18 U.S.C. § 2511 and § 2515. Some cases relating to these issues are *United States v. Jones*, 552 F.2d 661 (6th Cir. 1976); *United States v. Murdock*, 63 F.3d 1391 (6th Cir. 1987); and *Pollack v. Pollack*, 154 F.3d 601 (6th Cir. 1998). These statutes and the principles contained therein also apply to the interception of cell phone conversations. See, for example, *Schubert v. Metrophone*, 898 F.2d 401 (3d Cir. 1990).

Conclusion

Rather than make the attorney's life easier, the proliferation of electronic information has made it more difficult, especially in the areas of civil and criminal litigation. With a basic understanding of technology and certain basic principles, lawyers can reduce the time and expense (and danger) of obtaining and discovering electronic information. ■

Bill Ramsey is a partner in the Nashville firm of Neal & Harwell (ramseywt@nealharwell.com, 615-244-1713).

Phillip Hampton is a legal technologist and owner of LogicForce Consulting, LLC, specializing in providing computer forensic services, litigation and trial technology support, and electronic data discovery (615-238-3539, phampton@logicforce.com).

If a conversation is recorded without authority from any of the participants, the evidence is generally not admissible in court, and recording it is a crime. Similarly, it is against the law to intercept or obtain e-mail messages without authority.