



## ***Electronic Discovery and Evidence***

By Michael R. Arkfeld

REVIEWED BY MICHAEL COBLENZ

I know lawyers who print out every case-related e-mail they receive so that they can have a copy for their files, and I know lawyers who even have voice mail messages transcribed, but most people are not that obsessive about keeping records. They send emails, text messages, instant messages, voice mail and pager messages, and the like with little thought to whether there is any trace of the message as it goes through the ethers of cyberspace. But there are traces, and they can be useful evidence at trial.

Almost all business today is done on computers, and huge volumes of information are transferred over the Internet. This means that there is less evidence in paper form and more in electronic form. A number of recent high-profile cases have highlighted issues regarding electronic information. Monica Lewinsky's e-mails (which she thought she had deleted) led investigators to an infamous stained blue dress and the impeachment of a president. The investment house Merrill Lynch settled a multibillion-dollar security fraud case when the New York attorney general disclosed e-mails from securities analysts to stockbrokers describing the stocks the brokers were pushing as "garbage" and "dogs." These are just two examples of damaging evidence that the creator thought was lost forever in cyberspace.

If you litigate, you have undoubtedly dealt with some electronic discovery issues, most

commonly regarding e-mails and business records that exist almost entirely in electronic form. But these are just the tip of the digital iceberg.

Let me present a hypothetical example that I hope will make the issue a bit more interesting. Suppose you represent a client who claims her boss is sexually harassing her by sending her unwanted sexual text messages on her cell phone and instant messages on her computer. She also claims that on more than one occasion she has returned from lunch to find pornographic pictures on her computer and has heard her boss brag about his many conquests and state that he has them catalogued in his Palm Pilot. Of course, the boss denies all these allegations and even denies that he has ever looked at pornography on a computer. Can you get him? Is it possible to retrieve the messages or some record of his Web site visits? And if you can get them, can they be used at trial, either to prove harassment or to impeach character? Probably, but most lawyers will need some help with this kind of evidence.

Michael R. Arkfeld's *Electronic Discovery and Evidence* is a good place to start. It provides a readable introduction to the wide variety of electronic information that is floating around out there and that can be used as evidence. I listed a few examples in my hypothetical example, but Arkfeld discusses dozens more, including digital photos, Web site metatags, and data stored in flash memory, smart cards, caller ID, scanner and copier memory, Global Positioning System memory, and others.

There are really two issues that must be addressed when dealing with the discovery of electronic evidence: (1) technical aspects dealing with what constitutes electronic evidence, where it can be found, and how it can be technically retrieved; and (2) legal issues such as whether electronic data are legally discoverable, relevant, and admissible at trial. Arkfeld leads us through both topics but begins with a little historical and technical background. This discussion may be familiar to tech-savvy lawyers, but it is a valuable foundation for anyone else facing these issues.

In dealing with the technical aspects of electronic discovery, Arkfeld recommends that a lawyer seeking to discover esoteric electronic information (just about anything

beyond emails or files saved on the computer) obtain the assistance of a qualified technical expert. Deleted e-mails, for example, are often still located somewhere on the computer's hard drive, and a computer expert will be needed to go in and root them out. And even easily obtained data are likely to be stored in a format that most lawyers are not trained to interpret.

Knowing that the information is out there and that it is technologically obtainable is only part of the problem. To be usable, the information must be obtained through proper discovery methods. Chapter 6 of Arkfeld's book provides discovery pointers, and Chapter 7 discusses each of the federal discovery rules and describes how each can best be used to pry loose an opponent's electronic information. I should note at this point that the Committee on Rules of Practice and Procedure of the Judicial Conference of the

United States is currently debating changes to the federal rules to address the issue electronic information more thoroughly and to deal with the potentially costly burden of producing it.

Let's revisit my hypothetical example. Let's say that we've obtained the allegedly harassing boss's work and home computers, cell phone with a text-messaging feature, telephone company records, Internet service provider e-mail records, and the boss's personal digital assistant, such as Palm Pilot. Can any or all of these records be used at trial?

Chapter 8 leads us through the various admissibility issues - relevancy, hearsay, authentication - as they relate to electronic evidence. In my hypothetical case, sexually explicit propositions in e-mails, instant messages, or telephone text messages would be relevant evidence of sexual harassment. An attorney" could probably also impeach the boss by using the cookies on his computer that show frequent visits to pornographic Web sites.

But guess what? All this information is hearsay and will have to fall under one of the hearsay exceptions in order to be admissible at trial. And undoubtedly the boss's attorney will challenge the authenticity of the evidence. Thankfully, Arkfeld thoroughly addresses each issue and includes cites to reported cases dealing with these issues so

that the litigator can get started on that motion in limine.

Electronic evidence and discovery are very hot topics today. I receive flyers for books and classes on the subject almost weekly. If you're simply curious about the topic, go to a good CLE seminar. But if you litigate, you will need something more thorough - a resource that includes detailed legal and technical analysis of all the issues - and I certainly recommend Arkfeld's book for this purpose. It is a logical, thorough, and readable way for an attorney to prepare for the new world of electronic evidence and discovery. TFL

*Michael Coblenz is an intellectual property attorney in Lexington, Ky.*