

# TRIAL TIPS

## *Electronically Stored Information: A Primer for Litigators*

By Jules Epstein

### In less than a decade, judicial attitudes

toward and the litigator's reliance on electronically stored information (ESI) have changed dramatically. In 1999, judicial resistance to Web-page evidence that might have been "hacked" was so great as to exclude it outright; yet by 2007 its authenticity was deemed to be presumptively correct. The volume of data from electronic sources is so great that concern is now being expressed that discovery costs might limit access to the courts for many litigants. (See "The Big Data Dump," *The Economist*, August 28, 2008.)

To ensure admissibility of ESI, the capable litigator must focus on five issues: investigation, discovery, authentication, hearsay concerns, and the issue of "original writings."

Locating electronic evidence depends on several factors. If the investigator is a state official, her or his searches are cabined by Fourth Amendment strictures, while private actors are restricted by state privacy and electronic communications laws.

Once litigation has started, subpoena power and discovery tools come into play. Federal Rule of Civil Procedure 26(a) requires a party to disclose electronically stored information that the party may use to support its claims or defenses without awaiting a discovery request. The only limitations recognized are undue burden and cost.

Where the ESI is on the Internet, sophisticated search tools such as the "wayback machine" can be utilized. This program, available through the "Internet Archive" (<http://www.archive.org/web/web.php>), permits the user to see the content of a page on a particular date. Where the ESI is on a computer's hard drive, forensic software can search for deleted e-mails, Web-browsing history, and cached HTML pages.

Often critical to a search of ESI are the discovery and interpretation of metadata. Essentially a hidden set of codes, metadata can reveal file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification) and file permissions (e.g., who can read the data, who can write to it, who can run it). Where a computer shows no metadata, it may show that "anti-forensics" software has been used to delete or destroy data. A related set of data is "embedded information," such as a blind-copy address in an e-mail.

Once obtained, ESI evidence must be "authenticated." This may be done through a witness with knowledge who can identify the item(s); by establishing them as business records; by admission



or stipulation in civil proceedings; or by showing the information was generated by or with a process that produces reliable results.

Digital photographs are a case in point. Although easily subject to manipulation with readily available computer software programs, the image may be authenticated by the photographer or someone familiar with the scene depicted; and where the digital photo has been enhanced or is a converted image, testimony of an expert is an essential addition to explain the process used and the proven track record of generating reliable results.

The contents of the authenticated ESI will undoubtedly contain hearsay. This concern may be obviated by application of any number of hearsay exclusions or exemptions—the statement may be an admission of a party opponent; an excited utterance or present sense impression; a declaration of state of mind or one made for purposes of medical diagnosis or treatment; or a declaration against interest. Many ESI documents will be admissible as business records; others may be admissible as reports of government agencies.

After hearsay issues are resolved, the final evidentiary concern is the "original writings" requirement. Because the contents of the writing (e.g., the e-mail or Web page) are at issue, this rule requires production of an original. As duplicates are approved under the rule (Rule 1003, Fed.R.Evid.), however, this should rarely be a barrier to admission.

In sum, ESI offers a wealth of information. Its use depends on knowledgeable investigation and the recognition that introduction merely requires applying "old" rules of evidence to new forms of proof. ■



Jules Epstein is associate professor of law at Widener University School of Law, where he teaches Evidence and subjects in criminal law and procedure. Thanks are due to Adjunct Professor Richard Herrmann, who is Director of the Center for Law Practice Technology, a partner at Morris James in Wilmington, and a true expert in e-discovery, for his comments and assistance.