ITEM 9.06 | TEN PRACTICAL STEPS FOR HANDLING ELECTRONIC EVIDENCE[69]

1. Plan carefully to secure the client's relevant electronic evidence and to obtain evidence from the opponent or third parties. Electronically stored information (ESI) is volatile and may be altered, corrupted, or lost by human accident or error, by malicious intentional conduct, or through the automated operation of computers.

2. Plan carefully before and during discovery to obtain and to secure the foundation needed to admit evidence. Frequently, foundation is available in the form of metadata or other electronically stored information such as the file path, which may be available for a limited time and is volatile, alterable, or corruptible. Foundation may also be obtained through testimony or ancillary ESI or information about the equipment or software associated with the ESI. Many times such information or testimony is readily available only for a limited time. Plan for the admission of electronically stored information in the collection process. Manage the opposition so that the produced information will contain foundational information.

3. Request admission of the authenticity and admissibility of ESI whenever possible. Obtaining admissions on admissibility is not only economical; it saves drudgery and wasting of time during trial which can alienate the jury or judge.

4. When in doubt, err on the side of preservation. The scope of preservation and the timing of when preservation is triggered are based upon the circumstances of the case. Reasonable counsel may differ. However, the "down side" of potential sanctions against a client and attorney who fail to preserve electronic evidence or who engage in spoliation are universally less acceptable than the burden of preservation. If preservation appears overly burdensome, seek judicial assistance in advance under the doctrine of proportionality. Seeking forgiveness after destruction of evidence is not a reasonable strategy.

5. Use summaries and charts rather than voluminous printouts when presenting evidence to the trier of fact. The rules permit the admission of a summary document distilling of numerous and obscure documents into a cogent and organized chart if the chart is accurately based on admissible evidence, is introduced by a qualified witness and properly noticed, and will assist the trier of fact in understanding the evidence. Presenting important

evidence in organized form is much better than relying on a jury to locate information in a maze of exhibits.

6. Check public sources or social media. Information may be readily available from the Internet and especially social media. Valuable information may be retrievable outside formal discovery without alerting the opponent. When copying such media try to capture as much metadata as possible and document when the information was captured. The capture of a website as a PDF file will have its own metadata that may be used to demonstrate the capture time and date.

7. Use competent and effective witnesses to obtain publically available evidence. Frequently authentication of evidence will require a witness to testify about the manner in which the evidence was obtained and the device or software associated with the creation, modification, transmission, or storage of the ESI. Professional investigators with E-Discovery credentials and experience are good candidates for investigations of social networking websites, and conducting self-help E-Discovery. The receipt and management of ESI production from the opposition should be supervised by persons with adequate testifying witness skills.

8. Curb the client's self-help efforts by delineating strict boundaries of behavior. While self-help and self-collection may be desirable for the client economically, the client must understand the risks of inadequate of improper collections. An unbiased, technically competent expert may be the best person to collect the electronic evidence. A competent investigator can then authenticate the collected information at trial or hearings. In no case should the client illegally obtain evidence, misappropriate a password, or access information through subversion or artifice.

9. Advise the client of preservation obligations and warn against loss, alteration, or destruction of ESI. Sanctions can arise from behavior the client (or attorney) considers routine. For example, removing injudicious Facebook entries after preservation is triggered may be considered spoliation if a copy of the Facebook entries as they appeared before removal was not preserved.

10. Cooperate with opposing counsel concerning the admissibility of electronic evidence. All parties are well advised to exchange information and to anticipate and resolve by agreement as many electronic evidence issues as possible. The downstream costs associated with incorrect E-Discovery decisions and errors are substantial and occasionally case dispositive. Cooperation by

counsel on such matters is a sign of strength, professionalism, and competency.

Trial Lawyers Section of the Florida Bar
Conference of Circuit Court Judges
Conference of County Court Judges

Footnotes

[69] Artigliere, R. and Hamilton, W., LEXISNEXIS® PRACTICE GUIDE: FLORIDA E-DISCOVERY AND EVIDENCE, §1.05 (2015).