



CHAPTER IX
FLORIDA HANDBOOK ON CIVIL DISCOVERY PRACTICE (2016)
[ALL-IN-ONE DOCUMENT]

CHAPTER IX
ELECTRONIC DISCOVERY

E: TextBookDiscrimination@gmail.com
W: www.TextBookDiscrimination.com

visit TBD's [website](#) for the most up-to-date information

TABLE OF CONTENTS | CHAPTER IX | ELECTRONIC DISCOVERY

ID	Item	Title	Page
0900	9.00	Chapter 9 Intro	4
0901	9.01	Law, Policy, and Principles of Electronic...	11
0902	9.02	Framework for the Trial Lawyer Facing E-Discovery	14
0903	9.03	Duties of Attorney and Client Regarding...	18
0904	9.04	Florida's "Safe Harbor" Provision	25
0905	9.05	Collection and Review of ESI	26
0906	9.06	Ten Practical Steps for Handling Electronic...	28
0907	9.07	"Self-Help" Discovery	31
0908	9.08	Conferring with Opposing Counsel	34
0909	9.09	Inspection of Client Computers and Equipment	35
0910	9.10	Requesting Production and Making Production of ESI	38
0911	9.11	Production of ESI Pursuant to Subpoena	41
0912	9.12	Discovery of Social Medial ESI	43
0913	9.13	Conclusion	45
-	n/a	Appendix	46

2016 FLORIDA HANDBOOK ON CIVIL DISCOVERY PRACTICE

CHAPTER IX ELECTRONIC DISCOVERY

ITEMS: 9.00 through 9.13

ITEM 9.00 | CHAPTER 9 INTRO

Florida litigators increasingly confront discovery involving electronic documents and other types of electronically stored information ("ESI")¹ and the hardware and media on which ESI is created, transferred, communicated, and stored. Because far more than 95% of today's documents are created, transferred, or maintained electronically, and because computers, phones, and other electronic devices pervade our culture, e-discovery can crop up in almost any case from a simple negligence case to commercial litigation. The fundamental issues regarding ESI involve (1) disclosure and protection of client ESI and hardware, (2) preservation of ESI by the client and the opposing parties and third parties, (3) access to ESI of opposing parties and third parties, (4) maintaining privacy and privilege, (5) costs of discovery, and (6) application of Florida's existing discovery rules and common law in an arena that changes virtually every day as technology advances.

Competent representation of the client requires the legal skill, knowledge, thoroughness, and preparation necessary for the representation.² Competence in ESI discovery is essential to successfully manage such discovery in an effective, economical, efficient, and balanced fashion. Since the law lags behind emerging and changing technology and because of the increasing availability of discoverable ESI, it is incumbent on lawyers and judges to make special efforts to become competent and stay current on ESI fundamentals and discovery. Staying current entails up-to-date knowledge of the culture of information: how information is created, used, managed, stored, communicated, and manipulated. New technology and information cultures are rapidly evolving, including new types of social media, small personal computer devices such as watches, cloud storage websites of all kinds where information may be kept indefinitely, and even appliances such as online security systems that are part of what is called the Internet of Things. All of these new products and information sources can create relevant evidence in a variety of cases. The volume of potentially relevant electronic evidence also continues to increase at an exponential level.

One of the foremost challenges in this kind of complex environment is protection of the client's confidential information, included personal protected information and privileged communications. This requires counsel to ensure that client information is protected and is disclosed only to the extent required by law or reasonably

necessary to serve the client's interest.³ Court recordkeeping and filing is now done in electronic format in Florida courts. This makes unfettered third party electronic access to court records, including client information in the record, far easier than ever before. Accordingly, counsel should only put in the record that which is required or reasonably necessary to serve the client's interest. If necessary, invoke the process of sealing private or sensitive information before the record becomes available as a public record.⁴ In anticipation of electronic recordkeeping and the need for protection of privacy interests of parties and non-parties, the Florida Supreme Court enacted rules requiring lawyers to analyze and screen information for certain confidential information before it is placed in the court record.⁵ At a minimum, pursuant to Fla. R. Civ. P. 1.280(g), information should not be filed with the court absent good cause, which is satisfied only when the filing of the information is allowed or required by another applicable rule of procedure or by court order.⁶ The lawyer is obligated to know enough about the client's ESI and the locations where it may be found to fully comply with discovery without making unnecessary disclosures. The client's equipment, data, and software should be protected from damage or destruction. The client should also be fully informed on the extent, if any, of the obligation to preserve information. At the same time, the client's business processes and handling of data should be protected from unnecessary intrusion from perceived court-related obligations. Finally, counsel and the court should be sufficiently informed of the ESI technology systems likely to contain relevant information in order to assist counsel to obtain permitted discovery of ESI from the opposing party and third parties.

Rulemaking for electronic discovery nationwide and in Florida has lagged behind the technology of how data is created, stored, and communicated. Nonetheless, Florida Civil Procedure and Judicial Administration Rules now expressly address issues caused by the use of digital technology in Florida Courts⁷ and discovery of ESI.⁸ Effective September 1, 2012, the Florida Supreme Court adopted several amendments to the Florida Rules of Civil Procedure⁹ largely modeled on the 2006 Amendments to the Federal Rules of Civil Procedure.¹⁰ Compatibility with federal rules enables use of federal decisions on electronic discovery as persuasive authority¹¹ in the absence of Florida cases and ensures harmony of e-discovery law between cases in Florida state courts and cases in federal court and other states. The Florida electronic discovery rules contain some improvements and adjustments from their federal

counterparts that arguably make the rules better suited to the broader range of state court jurisdiction in size and subject matter. A chart comparing the Florida electronic rules and the federal rules is attached to this chapter as Appendix A.

There are many good reasons for specialized rules for ESI discovery. ESI is ephemeral; sometimes easily hidden, mislabeled, or destroyed; available from multiple sources in a variety of forms; capable of electronic search, analysis and compilation; sometimes accompanied by information or availability not apparent to the creator or user, such as metadata; and frequently misunderstood by persons lacking in expertise. ESI also exists in incredibly large quantities. One Thousand gigabyte (One Terabyte) computer hard-drives are now standard issue on many computers, whereas a single gigabyte of information is equivalent to a truckload of paper documents. Many people today receive hundreds of e-mails and text messages a day and they may store them indefinitely in a variety of locations, some of which may be unknown to them. It is not uncommon in business today for management personnel to each keep hundreds of thousands of emails and attachments. Large enterprises commonly store trillions of emails and attachments, and in many cases may have to search through millions of emails to try to locate relevant evidence. There are often accessibility problems for some of the ESI stored, including backup systems. The places on which ESI can be stored or located are manifold and ever changing, and include the over one-trillion websites that now exist on the Internet. ESI may sometimes be easier and cheaper to search and to produce in electronic form than the same quantity of paper documents, but it is often much more difficult to locate and retrieve relevant ESI. Again, that is largely because of the high volume of total ESI maintained on a multiplicity of systems that may contain relevant information. The problem is compounded by the need to review most of the material for privilege, privacy, and trade secrets before it is disclosed. For these reasons it is today far more difficult and more expensive to access, search, categorize, compile, and produce relevant ESI than in the past when most records were only in paper form, were easily organized and accessed in centralized locations, and were far, far fewer in number and type.

Issues related to the spiraling cost issues of e-discovery contribute to the special treatment for ESI provided in the new rules and case law. Florida rules expressly provide that ESI is discoverable,¹² but they also require proportionality of expense.¹³ Florida rules help maintain cost proportionality by providing an

express framework for dealing with issues of preservation, production, and protection for hard-to-find and retrieve ESI and the media, equipment, and third party Internet "cloud" storage websites that hold ESI.¹⁴ A person may object to discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of burden or cost. The person from whom discovery is sought has the initial burden of showing that the information sought or the format requested is not reasonably accessible because of undue burden or cost. If that showing is made by specific evidence, the court may nonetheless order the discovery upon a showing of good cause. The court may specify conditions of the discovery, including ordering that some or all of the expenses incurred by the person from whom discovery is sought be paid by the party seeking the discovery.¹⁵

In *Zubulake v. UBS Warburg LLC*, 217 FRD 309 (S.D.N.Y. 2003), the court set forth an analytical framework for determining whether it is appropriate to shift the costs of electronic discovery. If the responding party is producing data from "inaccessible" sources, i.e. data that is not readily useable and must be restored to an accessible format, the court identified seven factors to be considered in determining whether shifting the cost of production is appropriate.¹⁶

The scope of discovery may also be limited by the producing party or person's privacy rights, as when the relevance or need for the information requested does not exceed the privacy interests of the person or party from whom it is sought.¹⁷

Florida rules also provide additional protection for confidential and privileged information not discoverable that may be inadvertently produced with discoverable material.¹⁸ Rule 1.285, Florida Rules of Civil Procedure, establishes a process by which a party, person, or entity may retroactively assert privilege as to inadvertently disclosed materials, regardless of whether the inadvertent disclosure was made pursuant to "formal demand or informal request."¹⁹ The privilege must be asserted within ten days of actual discovery of the inadvertent disclosure by serving a prescribed written notice of the assertion of privilege on the party to whom the materials were disclosed.²⁰ A party receiving notice under Fla. R. Civ. P. 1.285(a) must promptly (1) return, sequester, or destroy the materials and any copies of the materials, (2) notify any other party, person, or entity to whom it has disclosed the materials of the fact that the notice has been served and of the effect of the rule, and (3) take reasonable

steps to retrieve the materials disclosed.²¹ Rule 1.285 prescribes the manner in which a receiving party may challenge the assertion of privilege²² and the effect of a court determination that privilege applies.²³

Because ESI and the modern equipment that creates, holds, communicates, or manipulates it are complex and constantly evolving, sometimes expert assistance is needed by clients, counsel, or the court to search and prepare ESI for production. Such expert assistance may involve legal as well as technical issues and tasks. The parties and Court should consider the appointment of Special Masters or Third Party Neutral experts in appropriate cases.

The developing principles for electronic discovery and the Committee Notes to the Florida Rules of Civil Procedure encourage cooperation and transparency by the parties during meetings between counsel early in a case to try to agree on the scope of preservation and discovery and methods of production.²⁴ Counsel are encouraged to bring any areas of disagreement to the courts for resolution early in a case. These issues may also be addressed in a Rule 1.200 or Rule 1.201 case management conference.²⁵ Specific mention of case management for electronically stored information is found in Rule 1.200, Fla. R. Civ. P.²⁶ and in Rule 1.201 for cases that are declared complex.²⁷ In resolving these disputes courts must balance the need for legitimate discovery with principles of proportionality and the just, speedy and efficient resolution of the case.²⁸

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

Footnotes

¹ Electronically stored information, “ESI,” is the nomenclature adopted in the Florida and federal rules to refer to computer files of all kinds. See Fla. R. Civ. P. 1.280(b)(3); Rule 34, Federal Rules of Civil Procedure. The term ESI is not defined in the Florida and federal rules on purpose because of the ever-changing nature of such information. The Comments to the Federal Rules explain that the term ESI should be construed expansively “to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.”

² Rule 4-1.1, Florida Rules of Professional Conduct. See also ABA Model Rules of Professional Conduct, Rule 1.1 Competence—Comment, Para. (8) found at <http://bit.ly/NZsya6>.

³ Rule 4-1.6, Florida Rules of Professional Conduct. See also Fla. Prof. Ethics Op. 10-2 (obligation of lawyers with regard to confidentiality of client information when employing devices with hard drives and other media); 06-2 (responsibility for confidentiality and other obligations regarding metadata).

⁴ Fla. R. Jud. Admin. 2.420.

⁵ Fla. R. Civ. P. 1.280(g); 1.310(f)(3); 1.340(e); 1.350(d); and Fla. R. Jud. Admin. 2.420; 2.425.

⁶ Rule 1.280(g) provides: “Information obtained during discovery shall not be filed with the court until such time as it is filed for good cause. The requirement of good cause is satisfied only where the filing of the information is allowed or required by another applicable rule of procedure or by court order. All filings of discovery documents shall comply with Florida Rule of Judicial Administration 2.425. The court shall have authority to impose sanctions for violation of this rule.”

⁷ Id.

⁸ See *In re Amendments to the Florida Rules of Civil Procedure -- Electronic Discovery*, 95 So. 3d 76 (Fla. 2012). See also Fla. R. Civ. P. 1.285 (inadvertent disclosure of privileged material). In addition, Florida's 9th, 11th, 13th, and 17th Circuits have business or commercial litigation sections with special local administrative rules and processes for more complicated cases. These local rules include special handling of electronically stored information. Refer to local rules and comply with all requirements when handling cases assigned to a special commercial or business court.

⁹ Id.

¹⁰ Fed. R. Civ. P. 16, 26, 33, 34, 37 and 45. The Federal Rules of Civil Procedure were amended, effective December 1, 2015.

¹¹ Federal courts have generated copious numbers of cases under the federal e-discovery rules since 2007, because federal district judges and magistrates regularly enter published discovery opinions and orders, which creates a body of useful written law that is largely absent in Florida state court.

¹² Fla. R. Civ. P. 1.280(b)(3) (“A party may obtain discovery of electronically stored information in accordance with these rules).

¹³ Fla. R. Civ. P. 1.280(d)(2)(ii) (“the court must limit the frequency or extent of discovery otherwise allowed by these rules if it determines that... the burden or expense of the discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.”).

¹⁴ Fla. R. Civ. P. 1.280(d)(2)(ii).

¹⁵ *Id.*

¹⁶ *Zubulake*, *id.*, 217 FRD at 322.

¹⁷ Compare *Root v. Balfour Beatty Const., LLC*, 132 So. 3d 867,869 (Fla. 2d DCA 2014) (order compelling the production of social media discovery that implicates privacy rights demonstrates irreparable harm), with *Nucci v. Target Corp.*, 162 So. 3d 146 (Fla. 4th DCA 2015) (photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established).

¹⁸ Fla. R. Civ. P. 1.285.

¹⁹ Fla. R. Civ. P. 1.285(a).

²⁰ *Id.* The notice must include specifics on the materials in question, the nature of the privilege asserted, and the date on which inadvertent disclosure was discovered. The process applies to any privilege cognizable at law, including the attorney-client, work product, and the several other types of privileges recognized in the Florida Evidence Code. See Fla. Stat. § 90.501–.510 (journalist, lawyer-client, psychotherapist-patient, sexual assault counselor-victim, domestic violence advocate-victim, husband-wife, clergy, accountant-client, and trade secret privileges). *Id.*

²¹ Fla. R. Civ. P. 1.285(b). Nothing in Rule 1.285 diminishes or limits any ethical obligation with regard to receipt of privileged materials pursuant to Fla. R. Prof. Conduct 4-4.4(b). *Id.*

²² Fla. R. Civ. P. 1.285(c).

²³ Fla. R. Civ. P. 1.285(d).

²⁴ See Fla. R. Civ. P. 1.280, 2012 Committee Notes (“The parties should consider conferring with one another at the earliest practical opportunity to discuss the reasonable scope of preservation and production of electronically stored information.”).

²⁵ See Fla. R. Civ. P. 1.280, 2012 Committee Notes.

²⁶ Fla. R. Civ. P. 1.200(a)(5)-(7).

²⁷ Fla. R. Civ. P. 1.201(b)(1)(J).

²⁸ Fla. R. Civ. P. 1.010; 1.280(d).

ITEM 9.01 | LAW, POLICY, AND PRINCIPLES OF ELECTRONIC DISCOVERY

The complexity in application of discovery rules and policies to ESI and hardware and media is creating a burgeoning body of common law, primarily in federal court.²⁹ Case law in Florida on this subject is currently limited, but useful.³⁰ Most importantly, current Florida civil procedure rules for e-discovery were developed by selecting the best of the federal rules and distilling Florida common law authority into practical and balanced rules appropriate for the wide array of types and size of cases in Florida state courts that apply the civil rules.³¹ The rules provide a useful framework for anticipating and addressing prominent e-discovery issues. Based on the similarity between Florida and federal rules, Florida trial courts are likely to refer to federal courts and the extensive body of case law in the federal system³² as well as cases arising in states with rules similar to Florida and federal rules. State court judges are also likely to be influenced by the publications of The Sedona Conference®,³³ a private research group of lawyers, judges and e-discovery vendors dedicated to the development of standards and best practices in this evolving field of law and policy. The Sedona Conference® writings have been widely cited in the federal courts, especially its Sedona Principles,³⁴ and Cooperation Proclamation.³⁵ Also especially helpful are its Glossary³⁶ of e-discovery related terms, and its commentaries on Search and Retrieval Methods,³⁷ Achieving Quality,³⁸ and Litigation Holds.³⁹ Many excellent text and trade publications, including free online resources, are also available.⁴⁰

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

Footnotes

²⁹ This chapter focuses on Florida state court e-discovery. Discussion of federal law herein is undertaken only because of the availability of federal law for guidance in state court cases and is not intended to provide practitioners with a manual for discovery in federal court cases. See *supra* n. 11.

³⁰ See, e.g., *Nucci v. Target Corp.*, *supra* n. 16 (no expectation of privacy in photos posted on Facebook regardless of privacy settings used by producing party); *Root v. Balfour Beatty Const., LLC*, *supra* n. 17 (privacy interest in Facebook postings upheld against overbroad request); *Antico v. Sindt Trucking, Inc.*, 148 So. 3d 163 (Fla. 1st DCA 2014) (access to decedent's iPhone granted to determine whether she was texting during automobile accident in which she was killed); *E.I. DuPont De Nemours & Co. v. Sidran*, 140 So. 3d 620, 650 (Fla. 3d DCA 2014) (sanctions not appropriate for fraud on the court in the manner in which ESI was collected and stored by defendant for discovery in multiple suits); *Osmulski v. Oldsmar Fine Wine, Inc.*, 93 So. 3d 389 (Fla. 2d DCA 2012), rev. den., 109 So. 3d 781 (Fla. 2013) (preservation obligations before case is filed are explained in this case); *Holland v. Barfield*, 35 So. 3d 2010 Fla. App. LEXIS 6293; 35 Fla. L. Weekly D 1018 (Fla. 5th DCA May 7, 2010) (order granting opposing expert in wrongful death case unrestricted access to review petitioner's hard drive and SIM card quashed as violative of privacy); *Menke v. Broward County School Board*, 916 So. 2d 8 (4th DCA 2005) (establishing basis and limits on access to opposing party's hardware in order to search for discoverable information); *Strasser II: Strasser v. Yalamanchi*, 783 So. 2d 1087 (Fla. 4th DCA 2001) (spoliation of electronic records); *Strasser I: Strasser v. Yalamanchi*, 669 So. 2d 1142 (Fla. 4th DCA 1996) (designating Florida procedural rules giving rise to discovery of ESI and the equipment that holds them and setting limits on scope of such discovery); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.* 2005 WL 674885, (Fla. Cir. Ct., 2005) (one of the best known e-discovery opinions in the country, primarily because the sanctions for ESI spoliation resulted in a default judgment for \$1.5 Billion. The judgment was reversed on other grounds).

³¹ See In re Amendments to the Florida Rules of Civil Procedure -- Electronic Discovery, *supra* n. 8.

³² See the following Federal Rules of Civil Procedure and accompanying rule commentary pertaining to the 2015 amendment: Rule 16(b), 26(a)(1)(B), 26(b)(2)(B), 26(f), 26(b)(5), 33, 34, 37(f) and 45. Also see the large and rapidly growing body of opinions by United States Magistrate Judges and District Court Judges in Florida and elsewhere around the country. Federal law is far more developed than Florida e-discovery law and provides useful guidance for lawyers and judges. That is not likely to change because Florida trial court decisions are seldom published.

³³ The Sedona Conference® publications are all available online without charge for individual use. See <http://www.thesedonaconference.org/>. As of 2013, judges have exclusive access to special judicial resources developed by The Sedona Conference® which are based on the aforementioned Sedona Principles and writings but tailored to the judicial perspective. Accordingly, lawyers who use, conform to, and cite pertinent materials from The Sedona Conference® will hopefully find judges enlightened on relevant policies and principles referenced *infra* notes 32-37.

³⁴ This can be downloaded after registration at: <http://www.thesedonaconference.org/dltForm?did=2007SummaryofSedonaPrinciples2ndEditionAug17as sent forWG1.pdf>.

³⁵ See "The Sedona Conference® Cooperation Proclamation," 10 Sedona Conf. J. 331 (2009 Supp.).

³⁶ http://www.thesedonaconference.org/dltForm?did=TSCGlossary_12_07.pdf.

³⁷

http://www.thesedonaconference.org/dltForm?did=Best_Practices_Retrieval_Methods_revised_cover_and_preface.pdf.

³⁸ http://www.thesedonaconference.org/dltForm?did=Achieving_Quality.pdf

³⁹ http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf.

⁴⁰ See e.g.: Ralph Losey's weekly blog: e-discovery team found at <http://www.e-discoveryteam.com> and his several books and law review articles on electronic discovery that are referenced there.

ITEM 9.02 | FRAMEWORK FOR THE TRIAL LAWYER FACING E-DISCOVERY

1. Familiarize yourself with the client's electronic records and computer systems used for storing this ESI, including how they are distributed, maintained, deleted, and backed-up. If the client has a routine destruction policy for hard copies, or also for ESI (and most companies now do), address the issue of preservation immediately. Failure to preserve records, including ESI, may result in severe sanctions for the client and possibly counsel.

2. Ensure that written preservation hold notices are provided by the client to any key players within their control that instructs them to preserve any potentially relevant ESI in their custody, and to not alter or destroy potentially relevant ESI pending the conclusion of the lawsuit. Notice should also be provided to third parties who are believed to hold or control ESI that is likely to be relevant to issues in the case. Counsel should follow-up on these written notices by prompt personal communications with key players, and then periodic reminder notices thereafter. Caution should be exercised is relying upon key players to locate or collect potentially relevant ESI. In some circumstances such self-collection should not be permitted, or should be supplemented by bulk collection of all the custodian's ESI. Today bulk collection of all a custodian's email within a certain date range is the rule in all but small cases. Keyword filtering of bulk collection is also disfavored in all but smaller cases because of the known unreliability of keywords and concern that important evidence will be omitted. Mistakes are easily made in ESI preservation and collection, and counsel has a personal duty to supervise the preservation, search and collection of potentially relevant ESI. If counsel is not competent to carry out these responsibilities in a particular matter, then they should affiliate with other counsel who are competent. The hiring of non-law firm vendors in e-discovery cannot discharge an attorney's duty of competence and personal responsibility.

3. Inform the client of all obligations for discovery by both sides and develop a plan to protect privileged or private information. Again, counsel should be actively involved in client's ESI preservation and collection efforts.

4. Work with the client and IT experts, if required, to develop a plan to collect and review ESI for possible

production, including a review for private, privileged, or trade secret information that may be entitled to protection from open disclosure. Determinations of responsiveness, relevance, or qualification for confidentiality or privilege protections should not be delegated to the client, IT expert, or vendor as these are uniquely legal determinations for which counsel is responsible.

5. Determine the preferred format to make and receive production of ESI, typically either in the original native format, which would necessarily include all internal metadata of a document, or in some type of flat-file type PDF or TIFF format, with a load file containing the file's internal metadata. Metadata is an inherent part of all ESI and should be included in most productions. The removal of internal metadata from a document, which would include such information as who created the document, the date of creation, last date it was accessed, blind copy of an email, and the like, constitutes an alteration of the original electronic version of that document and is typically not desired or necessary. If there is a particular type of metadata of concern to the requesting or responding party, specific requests or objections should be made.

6. Determine whether expert legal or technical assistance, or both, may be needed to sort out legal or practical issues involving ESI and its media or equipment. Reach out to opposing counsel early to attempt to coordinate and cooperate on technical issues and set up lines of communication and cooperation between the IT technicians that may be retained by both sides to assist in the e-discovery efforts. It may be appropriate for the parties to retain third-party neutral experts in some cases with unusual or complex technical issues, or other e-discovery challenges, such as search of large disorganized collections of ESI.

7. Find out what information may be discoverable from the opponent and seek disclosure of their preservation efforts and intended production formats, and what ESI they will seek discovery of, including their metadata demands, if any. Send a request for the opponent to preserve electronically stored information as soon as possible and include a formal discovery request for such information at the earliest possible date.⁴¹

8. Evaluate the reasonability and suitability of the opponent's preservation, collection, and production plans,

including any search or production issues, and attempt early resolution of any disputes. This should be accomplished before any large productions are actually made so as to avoid expensive do-overs. Beware of preservation, collection, and search based on keyword matching alone. This approach is frequently ineffective and far better technological solutions are now available.⁴² When keyword terms are used as part of a search and review protocol they should always be carefully tested, and should never be negotiated in the blind based on mere intuition by counsel that they will include most of the relevant evidence.

9. Determine whether discoverable ESI is available from multiple sources, including third parties. Frequently ESI documents, such as e-mail or draft contracts that have been communicated to or handled by multiple parties will contain useful additional or even conflicting information. Some sources of information are more accessible than others, meaning they are easier or less costly to access. Upon a proper showing under the rules, parties must be required to obtain information from the least burdensome source, and the court must limit unreasonably cumulative or duplicative discovery.⁴³

10. Weigh the cost of ESI discovery and determine whether costs may be shifted to protect the client or whether the cost of discovery outweighs the potential benefit.⁴⁴

11. Electronic discovery is typically conducted in phases wherein the most easily accessible and likely relevant ESI are searched and produced first, and then the necessity for further discovery is evaluated. Limiting factors for the first pass include accessibility, date range, custodians, volume, and secondary ESI storage.

12. Ensure to the extent possible that the value of the discovery sought and produced is proportional in the context of the case at hand.⁴⁵

13. If any of the foregoing steps require expert consultation or assistance, find a suitable expert and involve the expert early enough in the process that preservation obligations for the client and opponent are timely invoked.⁴⁶ Again, parties should consider the advisability of sharing a neutral third-party expert, which can realize substantial cost and time savings.

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

Footnotes

⁴¹ *Osmulski*, supra n. 29 (preservation obligations may occur before case is filed).

⁴² *William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. 2009); Losey, R. *Adventures in Electronic Discovery, Chapter Child's Game of "Go Fish" is a Poor Model for e-Discovery Search*, (West Thomson Reuters, 2011); *Da Silva Moore v. Publicis Groupe*, 2012 WL 607412 (S.D.N.Y. Feb. 24, 2012).

⁴³ Fla. R. Civ. P. 1.280(d) (the court must limit the frequency or extent of discovery otherwise allowed by these rules if it determines that the discovery sought is unreasonably cumulative or duplicative, or can be obtained from another source or in another manner that is more convenient, less burdensome, or less expensive).

⁴⁴ Fla. R. Civ. P. 1.280(d)(1); (d)(2).

⁴⁵ Fla. R. Civ. P. 1.280(d)(2)(ii).

⁴⁶ For preservation triggers, see *Osmulski*, supra n. 29; *Gayer v. Fine Line Constr. & Elec., Inc.*, 970 So. 2d 424, 426 (Fla. 4th DCA 2007).

ITEM 9.03 | DUTIES OF ATTORNEY AND CLIENT REGARDING PRESERVATION OF ESI

Electronically stored information is by its very nature ephemeral and easily transportable, so it can be instantaneously lost, altered, destroyed, or hidden. Understanding the duties regarding preservation of evidence is vital to those who possess or control evidence and those who seek to use it in litigation.⁴⁷ The Florida state court common law of preservation is unique⁴⁸ and somewhat unsettled, increasing the challenge for lawyers advising their clients on preservation duty. In general, a duty to preserve in Florida can arise from many sources, including court orders, subpoenas, government regulations, statutes, contracts, discovery requests, and common law. Some Florida courts have held that a duty to preserve evidence is triggered by contract, by statute, or by a properly served discovery request once a lawsuit has already been filed.⁴⁹ In fact, a number of Florida cases have expressly held that, absent a contractual or statutory duty, there is no duty to preserve evidence before litigation commences.⁵⁰ However, a few Florida cases somewhat inconsistently appear to recognize a pre-suit obligation to preserve evidence where the party controlling evidence can reasonably foresee a claim and the relevance of the evidence.⁵¹ For counsel advising clients on preservation duty, notwithstanding these conflicts, or perhaps because of them, it makes sense to advise the client to preserve rather than dispose of relevant evidence, even if suit has not been filed. First, some cases may be filed in either state or federal court, and reliance on a perceived lack of pre-suit duty to preserve under Florida law will not succeed in federal court where the duty to preserve is triggered when litigation is reasonably anticipated. Second, there may be a statutory or contractual obligation to preserve that is not apparent at the time advice is rendered. Third, a finding of spoliation against client or counsel is indeed a serious outcome and may have ramifications beyond the case at issue.

A common e-discovery issue for parties and counsel is the "scope" of evidence that must be preserved. Virtually all cases involve decision-making on the time frame for preservation, the substantive content which determines whether documents are relevant, and the breadth of places in which relevant evidence may be found. In large cases, parties may delineate preservation by persons who are likely to have relevant information, often called "custodians" as they have personal custody of the ESI by virtue of it being their email account, text message account, etc.

The very breadth of reasonably required preservation may raise issues of burden and cost. However, in applying proportionality to limit discovery duties, counsel must be careful to distinguish between scope of preservation versus scope of production. Preservation occurs at a point in time in which potential issues may not be crystallized and the relevance of certain documents may be fuzzy or indeterminable. Counsel and parties should usually err on the side of preservation, at least until the relevance picture sufficiently clarifies to safely distinguish that which must be preserved and produced. While some federal cases have expressed the principle that scope of preservation efforts may be guided by reasonableness and proportionality,⁵² other federal courts disagree.⁵³ In any event, counsel should advise a client to put a litigation hold in place and undertake reasonable efforts to identify and preserve evidence that is relevant by discovery standards.⁵⁴

As for counsel's duties with regard to preservation of evidence, the seminal federal case was written by Manhattan District Court Judge, Shira Scheindlin. It is actually a series of opinions written in the same case, collectively known as Zubulake, after the plaintiff, Laura Zubulake. There are four key opinions in this series.⁵⁵ These decisions are widely known by both federal and state judges and practitioners around the country.

Judge Scheindlin's last opinion, Zubulake V, has had the greatest impact upon federal courts and is also starting to have an impact on state courts, including Florida. In Zubulake V, Judge Scheindlin held that outside legal counsel has a duty to make certain that their client's ESI is identified and placed on hold. This new duty on attorneys was created because of the unusual nature and characteristics of ESI and information technology systems in which ESI is stored. Unlike paper documents, ESI can be easily modified or deleted, both intentionally and unintentionally. In many IT systems, especially those employed by medium to large size enterprises, ESI is automatically and routinely deleted and purged from the IT systems. Special actions must be taken by the client with such IT systems to suspend these normal ESI deletion procedures after litigation is reasonably anticipated.

Here are the words of Judge Scheindlin in Zubulake V that have frequently been relied upon to sanction attorneys who either unwittingly, or sometimes on purpose, failed to take any affirmative steps to advise and supervise their clients to stop the automatic destruction of ESI:

Counsel must become fully familiar with their client's documents retention policies as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system wide back up procedures in the actual (as opposed to theoretical) implementation of the firm's recycling policy it will also involve communicating with the key players in the litigation, in order to understand how they store information.⁵⁶

Of course, a party to litigation has a duty to preserve evidence in all forms, paper or ESI, and the bad faith failure to do so may constitute actionable spoliation. This is nothing new.⁵⁷ But the extension of this duty to the litigants' outside legal counsel in *Zubulake V*, which is sometimes called the "Zubulake Duty," is fairly new and controversial.⁵⁸ Although the "Zubulake Duty" has been accepted by many federal judges in Florida and elsewhere, it is unknown whether Florida state court judges will also impose such a duty upon attorneys. However, in view of the popularity in the federal system of placing this burden on the counsel of record, a prudent state court practitioner should also assume that they have such a duty.⁵⁹ Outside legal counsel should be proactive in communicating with their client and otherwise taking steps to see to it that the client institutes a litigation hold. Obviously, Judge Scheindlin does not intend to convert attorneys into guarantors of their client's conduct. She also notes in *Zubulake V* that if attorneys are diligent, and they properly investigate and communicate, they should not be held responsible for their client's failures:

A lawyer cannot be obliged to monitor her client like a parent watching a child. At some point, the client must bear responsibility for a failure to preserve.⁶⁰

However, counsel is obligated to have sufficient knowledge of client's IT systems to allow counsel to competently supervise the client's evidence preservation efforts, or lacking such knowledge and competence, should retain experts who do.

The duty to preserve of client and counsel requires a corporate client in most circumstances to provide a written litigation hold notice to its employees who may be involved in the lawsuit, or who may otherwise have custody or control of computers and other ESI storage devices with information relevant to the lawsuit. The notice should instruct them not to alter or destroy such ESI. The potential witnesses to the case should be instructed to construe

their duty to preserve ESI broadly and reminded that the ESI may be located in many different computers and ESI storage systems, including for instance, desktop computers, laptops, server storage, CDs, DVDs, flash drives, home computers, iPods, iPads, iPhones, blackberries, Internet storage webs (cloud computing), social media accounts, Internet e-mail accounts, voice mail, etc. The client's IT department or outside company should also be notified and instructed to modify certain auto-deletion features of the IT system that could otherwise delete potentially relevant evidence. In some cases, it may also be necessary to preserve backup tapes, but this is generally not required, especially if the relevant information on the tapes is likely just duplicative.⁶¹

There should be reasonable follow-up to the written notice, including conferences with the key players and IT personnel.

Judge Scheindlin wrote another opinion on the subject of litigation holds and ESI spoliation, which she refers to as her sequel to Zubulake.⁶² Pension Committee provides further guidance to federal and state courts on preservation issues, and the related issues of sanctions. Judge Scheindlin holds that the following failures to preserve evidence constitute gross negligence and thus should often result in sanctions of some kind:

After a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant Zubulake opinion in July, 2004, the following failures support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold, to identify the key players and to ensure that their electronic and paper records are preserved, to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control, and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

Judge Scheindlin goes on to hold that "parties need to anticipate and undertake document preservation with the most serious and thorough care, if for no other reason than to avoid the detour of sanctions."⁶³ Counsel should document their efforts to prove reasonableness in the event mistakes are made and relevant ESI deleted, despite best efforts. In any large ESI preservation,

collection and production, some errors are inevitable, and Judge Scheindlin notes this on several occasions in Pension Committee, including the opening paragraph where she observes:

In an era where vast amounts of electronic information is available for review, discovery in certain cases has become increasingly complex and expensive. Courts cannot and do not expect that any party can meet a standard of perfection.

This is an important point to remember. The volume and complexity of ESI makes perfection impossible and mistakes commonplace. All that Judge Scheindlin and other jurors and scholars in this field expect from the parties to litigation and their attorneys are good faith, diligent, and reasonable efforts. In Pension Committee, Judge Scheindlin found that the parties did not make reasonable diligent efforts, and so entered sanctions against them with the words:

While litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation. All of the plaintiffs in this motion failed to do so and have been sanctioned accordingly.

The opinion of Judge Scheindlin in Zubulake V and the Pension Committee cases provide a road map to practitioners on what needs to be done in order to preserve ESI from destruction, either intentional or accidental, and so avoid sanctions for spoliation. These and hundreds of other cases like it in the federal system are quite likely to be referred to and cited in state court proceedings. Although none of these federal cases are binding upon state court system, many judges find them persuasive, and the federal cases will often at least provide a starting point for further argument.

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

Footnotes

⁴⁷ Loss of evidence can be devastating to the party whose case would benefit from lost evidence; but a person or party holding relevant evidence make likewise suffer through sanctions if the evidence is lost or destroyed.

⁴⁸ Florida law on triggering of the duty to preserve is unlike federal court law and virtually every other state court jurisdiction. In federal court, and in many other jurisdictions, a party in control of relevant evidence is obligated to preserve it if there is reasonable anticipation of litigation.

⁴⁹ See, e.g., *Royal & Sunalliance v. Lauderdale Marine Center*, 877 So. 2d 843, 845 (4th DCA 2004).

⁵⁰ Id. (holding that "we find Royal's argument that there was a common law duty to preserve the evidence in anticipation of litigation to be without merit"); *Gayer v. Fine Line Constr. & Electric, Inc.*, supra n. 45 at 426 (Fla. 4th DCA 2007)(holding that "[b]ecause a duty to preserve evidence does not exist at common law, the duty must originate either in a contract, a statute, or a discovery request"); *In re: Electric Machinery Enterprises, Inc.*, 416 B.R. 801, 873 (M.D. Fla. 2009)("The majority of Florida courts have held that there is no common law duty to preserve evidence before litigation has commenced").

⁵¹ See *Osmulski*, supra n. 29 at 393, citing *American Hospitality Management Co. of Minnesota v. Hettiger*, 904 So. 2d 547, 549 (Fla. 4th DCA 2005)(where a defendant has evidence within its control, it can "be charged with a duty to preserve evidence where it could reasonably have foreseen the [plaintiff's] claim."). This is also the federal rule on when a duty to preserve is triggered.

⁵² See, e.g., *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 523 (D. Md. Sep. 9, 2010); *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010)("Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done--or not done--was proportional to that case and consistent with clearly established applicable standards").

⁵³ *Orbit One Communications, Inc. v. Ronsen*, 271 F.R.D. 429; 2010 U.S. Dist. LEXIS 123633 (S.D. N.Y. 2010)("Although some cases have suggested that the definition of what must be preserved should be guided by principles of "reasonableness and proportionality," [citations to Victor Stanley and Rimkus omitted], this standard may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle.").

⁵⁴ Information on preservation advice and litigation holds in Florida state court litigation is found in Ch. 5, *Initial Procedures in EDiscovery and Preservation of Evidence in Florida State Court*, Artigliere & Hamilton, LexisNexis Practice Guide Florida EDiscovery and Evidence, LexisNexis/Matthew Bender (2012) available from LexisNexis and from The Florida Bar.

⁵⁵ *Zubulake v UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (*Zubulake III*); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*); and *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake V*).

⁵⁶ *Zubulake V*, supra n. 54 at 432.

⁵⁷ See *Martino v. Wal-Mart Stores, Inc.*, 908 So. 2d 342 (Fla. 2005); *Golden Yachts, Inc. v. Hall*, 920 So. 2d 777, 781 (Fla. 4th DCA 2006).

⁵⁸ See *Metro. Opera Ass'n Inc. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union*, 212 F.R.D. 178, 218-219 (S.D.N.Y. 2003); but see Thomas Allman, *Deterring E-Discovery Misconduct By*

Counsel Sanctions: The Unintended Consequences of Qualcomm v. Broadcom, 118 Yale L.J. Pocket Part 161 (2009).

⁵⁹ Like their federal counterparts, Florida judges have statutory, rule-based, and inherent authority to sanction parties and their counsel for discovery violations and for spoliation. Judges are taught to seek out the source of the problem and administer a measured sanction that remedies the wrong committed. If the party is not the culprit, it makes little sense to administer the sanction against an innocent participant. See *Ham v. Dunmire*, 891 So. 2d 492, (Fla. 2004)(dismissal based solely on an attorney's neglect in a manner that unduly punishes a litigant espouses a policy that the Supreme Court of Florida does not wish to promote). Florida courts are not averse to applying appropriate sanctions to counsel. *Id.* at 498 (a trial court "unquestionably has power to discipline counsel" for discovery violations).

⁶⁰ *Zubulake V*, supra n. 54 at 433.

⁶¹ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (*Zubulake IV*); also see Rule 37(e) Federal Rules of Civil Procedure.

⁶² *The Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities, et al.*, 2010 WL 184312, 2010 U.S. Dist. LEXIS 4546 (S.D.N.Y. Jan. 15, 2010).

⁶³ *Id.*

ITEM 9.04 | FLORIDA'S "SAFE HARBOR" PROVISION

Many organizations have standard policies and procedures by which outdated and unnecessary electronically stored information is routinely deleted for purposes of economy, efficiency, security, or other valid business or organizational purposes. Florida followed the lead of the federal rules⁶⁴ by adopting a safe harbor provision to clarify that a party should not be sanctioned for the loss of electronic evidence due to the routine, good-faith operation of an electronic information system.⁶⁵ The existence of a "good faith" component prevents a party from exploiting the routine operation of an information system to thwart discovery obligations by allowing that operation to destroy information that party is required to preserve or produce. In determining good faith, the court may consider any steps taken by the party to comply with court orders, party agreements, or requests to preserve such information.⁶⁶

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

Footnotes

⁶⁴ Fed. R. Civ. P. 37(e) (2006). The federal rule has been amended, effective December 1, 2015.

⁶⁵ Fla. R. Civ. P. 1.380(e).

⁶⁶ Fla. R. Civ. P. 1.380 Committee Notes, 2012 Amendment.

ITEM 9.05 | COLLECTION AND REVIEW OF ESI

After counsel and litigants are satisfied the ESI has been preserved from destruction, and often as part of those efforts, the potentially relevant ESI should then be carefully collected. This requires copying of the computer files in a manner that does not alter or delete relevant information, which typically includes the metadata in or associated with the ESI (such as file name). Self-collection by the custodians themselves may be a dangerous practice in some circumstances due to their technical limitations and increased risk of accidental or intentional deletion of electronic evidence.⁶⁷ They are, for instance, quite likely to unintentionally change a computer file's metadata since opening a file, or simple copying of a file, will usually change many metadata fields. These altered metadata fields may prove of importance to the case. They are also likely to have a wrong understanding of what documents might be relevant for discovery purposes, typically adopting an over-narrow construction or otherwise not understanding the meaning of legal relevance. Also, as mentioned, keyword search based collection is hazardous, and should be avoided unless necessary in small cases for proportionality purposes to reduce the expense of review.⁶⁸ When keywords are used, they should be carefully tested in advance to evaluate efficacy and multiple refinements should be considered, typically Boolean logic combinations (and, or, but not, within a certain number of words, etc) and parametric limitations (keywords in specific fields of a document, as opposed to anywhere).

After collection, the ESI is typically processed to eliminate redundant duplicates and prepare the ESI for viewing. Full horizontal deduplication across all custodians is now typically used in all matters. The ESI is then searched for relevancy, and the smaller subset of potentially relevant ESI is then reviewed for final relevancy determinations as well as for privilege and confidentiality. Only after this review is production made to the requesting party.

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

Footnotes

⁶⁷ *National Day Laborer Organizing Network et al. v. United States Immigration and Customs Enforcement Agency, et al.*, 2012 U.S. Dist. Lexis 97863 (SDNY, July 13, 2012) (J. Scheindlin).

⁶⁸ See n. 41 *supra*.

ITEM 9.06 | TEN PRACTICAL STEPS FOR HANDLING ELECTRONIC EVIDENCE⁶⁹

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 or 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).

ITEM 9.07 | "SELF-HELP" DISCOVERY

Self-help discovery refers to the informal search and collection of electronically stored information outside the formal discovery process. Valuable information may be accessed without alerting the opponent or witnesses from whom or about whom the information is collected. A simple example of self-help discovery is obtaining information available on the internet about a party, witness, opposing counsel, issue in the case, industry or organization, or obtaining facts pertaining to the case. Using a Google or other search engine or a service or accessing social media⁷⁰ to get publicly available information through self-help methods can be cost-effective if properly done, but there are some caveats and cautions.

As with any collection of ESI for use in litigation, copying of the computer files should be done in a manner that does not alter or delete relevant information, such as contextual material or the metadata in or associated with the ESI. Self-collection by attorneys, attorney staff, or clients may be a dangerous practice due to technical limitations and increased risk of accidental or intentional deletion of electronic evidence. Further, the person who searches, finds, and collects information may end up being a witness to introduce the information. If the information is important enough to the litigation, it should be properly collected, stored, and preserved properly, and the collection should include information necessary for ultimate introduction of the ESI into evidence. This may require sophisticated or expert involvement.

Example: In an employment case, your employee client finds a government website that contains data in a spreadsheet form about the employer's industry that are relevant to issues in the case. The client takes a "screenshot" of the portions of the spreadsheet that apply to the employer and brings it to you. You put the information in your file in paper form for potential use in the case. What other steps may be considered with regard to this evidence? Answer: At this point, the file contains essentially a "picture" of a portion of ESI, so the client may ultimately need to testify at a minimum that the screenshot is a true and accurate depiction of what appeared on the website on the date and time of the screenshot. The client as well as the completeness and accuracy of the document are subject to challenge and cross-examination unless there is an admission on authenticity or admissibility from the opposing party. Spreadsheets may contain metadata, internal

calculations, footnotes, and other information that may be essential to the case. The data on the government website may change at any time or may not otherwise be available in the future, so a full and proper collection should be done right away by a sophisticated person, including contextual information and metadata. If necessary, use competent and effective witnesses to obtain publically available evidence. Proper collection, storage, and preservation of databases and spreadsheets can be technically challenging.

Self-help collection of information that is not clearly public information can be problematic. Self-help is only productive if it is done within the law.⁷¹ Efforts to access a computer or device of a party or witness or a person's email account may lead to sanctions or challenges on admissibility⁷² and potential disqualification of counsel in egregious cases, as where counsel has accessed privileged documents of the opposing party.⁷³ One basis for disqualification counsel is if counsel has obtained privileged documents of the opposing party.⁷⁴

Social media is a prolific source of information and a potential candidate for self-help discovery. Counsel should be familiar with the technology and characteristics of social media so as to be able to properly find, collect, and preserve information. For example, if discretion is needed when getting information from a party or witness' LinkedIn account, it is important to know that the target person will know who viewed their account unless the requesting person's LinkedIn settings are set to not disclose such access. Another example involves privacy settings on Facebook. Only limited information is available about a Facebook subscriber except for persons accepted as "Friends." However, it may be unethical to "Friend" an opposing party or witness for the sole purpose of extracting additional information from them on Facebook.⁷⁵ It may be necessary to request information subject to Facebook privacy settings through formal rather than self-help discovery.⁷⁶

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

Footnotes

⁷⁰ See DISCOVERY OF SOCIAL MEDIA ESI *infra*.

⁷¹ *O'Brien v. O'Brien*, 899 So. 2d 1133, 1137–38 (Fla. 5th DCA 2005)(where wife installed spyware on her husband's computer and retrieved the husband's on-line chats with other women, the trial judge correctly ruled that the evidence was not admissible because the conversations were illegally intercepted under the **Security of Communications Act**, Fla. Stat. § 934.03).

⁷² *Id.* Attorneys implicated in such improper behavior may be subject to discipline. *Fla. Bar v. Black*, 121 So. 3d 1038 (Fla. 2013)(attorney reprimanded for obtaining and keeping opposing party's iPhone which contained confidential and privileged information).

⁷³ *Castellano v. Winthrop*, 27 So. 3d 134 (Fla. 5th DCA 2010)(attorney disqualified after client illegally obtained opposing party privileged information and provided it to her attorney). The assessment and remedies vary depending on the findings and circumstances of the case after an evidentiary hearing to determine (1) whether counsel for a party possessed privileged materials, (2) the circumstances under which disclosure occurred, and (3) whether obtaining the privileged materials gave counsel an unfair advantage on material matters in the case. *Id.*

⁷⁴ *Id.*

⁷⁵ See *The Philadelphia Bar Assoc. Professional Guidance Committee*, *Op.* 2009-2 (Mar. 2009). Presumably the decision in Florida would be the same under Florida Rules. See Fla. R. of Prof. Cond. 4-4.1 (Truthfulness in Statements to Others) and 4-4.4 (Respect for Rights of Third Persons).

⁷⁶ Nucci, *supra* n. 16 (a personal injury case plaintiff's photographs on Facebook are discoverable regardless of privacy settings because there is no expectation of privacy for such information posted to others on Facebook).

ITEM 9.08 | CONFERRING WITH OPPOSING COUNSEL

Counsel are well advised to speak with each other at the commencement of the case concerning the preferred methods and format of production,⁷⁷ including topics as to what metadata fields are desired by the requesting party and the proposed preservation, culling, and search methods. Counsel should also discuss confidentiality concerns and attempt to reach agreement on these issues, as well as the related issues concerning the consequences of the inadvertent disclosure of privileged information. It is now common in the federal system for parties to enter into "Claw-Back" agreements protecting both sides from waiver from unintentional disclosure.⁷⁸ Florida now has a nearly identical rule that went into effect on January 1, 2011, in the form of Rule 1.285, Florida Rules of Civil Procedure (Inadvertent Disclosure of Privileged Materials). Clawback Agreements under the Florida Rule are anticipated and should be encouraged by courts and strengthened by court order. Since these agreements and protections are completely reciprocal, it is difficult to foresee legitimate grounds for opposition to this important safety net.

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

Footnotes

⁷⁷ See Rule 34(b)(2), Federal Rules of Civil Procedure, governing form of production. This essentially requires production of ESI in its original native format, or in another "reasonably useable" format, at the producer's choice, unless the request specifies the form.

⁷⁸ See Rule 26(b)(5)(B), Federal Rules of Civil Procedure, and Rule 502, Federal Rules of Evidence.

ITEM 9.09 | INSPECTION OF CLIENT COMPUTERS AND EQUIPMENT

One important issue in e-discovery concerning the limits on forensic examinations of a party's computers has already been addressed in Florida.⁷⁹ It follows without discussion, or much mention, a large body of federal and foreign state case law on the subject. Menke holds consistent with this law and protects a responding party from over-intrusive inspections of its computer systems by the requesting party.⁸⁰ The law generally requires a showing of good cause before such an inspection is allowed. The rules, both state and federal, only intend for parties, or third-parties, to make production of the ESI stored on electronic devices, not the devices themselves. This is a common novice mistake. Generally, the actual devices are only subject to inspection in unusual cases where you can prove that the party's search and production has not been reasonably or honestly performed or other even more rare circumstances.⁸¹ The background and reasoning for this law are set out well in Menke:

Today, instead of filing cabinets filled with paper documents, computers store bytes of information in an "electronic filing cabinet." Information from that cabinet can be extracted, just as one would look in the filing cabinet for the correct file containing the information being sought. In fact, even more information can be extracted, such as what internet sites an individual might access as well as the time spent in internet chat rooms. In civil litigation, we have never heard of a discovery request which would simply ask a party litigant to produce its business or personal filing cabinets for inspection by its adversary to see if they contain any information useful to the litigation. Requests for production ask the party to produce copies of the relevant information in those filing cabinets for the adversary.

Menke contends that the respondent's representative's wholesale access to his personal computer will expose confidential communications and matters entirely extraneous to the present litigation, such as banking records. Additionally, privileged communications, such as those between Menke and his attorney concerning the very issues in the underlying proceeding, may be exposed. Furthermore, Menke contends that his privacy is invaded by such an inspection, and his Fifth Amendment

right may also be implicated by such an intrusive review by the opposing expert.⁸²

The appeals court agreed with Menke and granted certiorari to quash the administrative law judge's order requiring production of Menke's computers. The court held that production and search of a computer is to be conducted by the producing party so as to protect their confidential information. Menke suggests that the production of the computer itself is a last resort only justified "in situations where evidence of intentional deletion of data was present."⁸³ The Menke court concluded with these words, which also seem a good note on which to end this article:

Because the order of the administrative law judge allowed the respondent's expert access to literally everything on the petitioner's computers, it did not protect against disclosure of confidential and privileged information. It therefore caused irreparable harm, and we grant the writ and quash the discovery order under review. We do not deny the Board the right to request that the petitioner produce relevant, non-privileged, information; we simply deny it unfettered access to the petitioner's computers in the first instance. Requests should conform to discovery methods and manners provided within the Rules of Civil Procedure.

Disclosure of confidential information is not the only potential harm when a party is permitted access to the opposing party's computers. Another consideration relating to a request for access to the client's computers, equipment, or software is the potential of harm to the client's hardware, software, and data. Any foray permitted by the court must balance the need for the level of access sought versus the potential harm to the party producing access. This is another reason for using neutral, qualified experts to assist in discovery.

One infrequent exception to the high bar protecting access to a party's computer or personal device may be when there is a showing that the device may contain relevant information, and there is no less intrusive means of discovery other than access to the device. In *Antico v. Sindt Trucking, Inc.*,⁸⁴ evidence was presented in a wrongful death auto negligence case that showed that the decedent-driver was texting or talking on her iPhone at the time of the automobile accident at issue in the case. Over vague "privacy" objections, the trial judge ordered that the defense (requesting

party) expert could examine the information on the decedent's iPhone over a 9-hour period around the accident, but the order strictly controlled how the confidential inspection must proceed.⁸⁵ The first district upheld the order as a proper balance of the need for the discovery and protection of privacy interests.⁸⁶ However, the decision of the appellate court was apparently influenced by the plaintiff's failure to advance any less intrusive alternatives for discovery than access as prescribed by the trial court.⁸⁷

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

Footnotes

⁷⁹ *Menke v. Broward County School Board*, 916 So. 2d 8 (Fla. 4th DCA 2005).

⁸⁰ See: *Peskoff v. Faber*, 2008 WL 2649506 (D.D.C. July 7, 2008); *Bro-Tech Corp. v. Thermax, Inc.*, 2008 WL 724627 (E.D. Pa. March 17, 2008); *Sterle v. Elizabeth Arden, Inc.*, 2008 WL 961216 (D. Conn. Apr. 9, 2008); *Xpel Technologies Corp. v. Am. Filter Film Distribs*, 2008 WL 744837 (W.D. Tex. Mar. 17, 2008); *Henry v. Quicken Loans, Inc.*, 2008 WL 474127 (E.D. Mich. Feb. 15, 2008); *In re Honza*, 2007 WL 4591917 (Tex. App. Dec. 28, 2007); *Coburn v. PN II, Inc.*, 2008 WL 879746 (D. Nev. Mar. 28, 2008); *Ferron v. Search Cactus, LLC*, 2008 WL 1902499 (S.D. Ohio Apr. 28, 2008); *Johnson v. Wells Fargo Home Mortgage, Inc.*, 2008 WL 2142219 (D. Nev. May 16, 2008); *Anadarko Petroleum Corp. v. Davis*, 2006 WL 3837518 (S.D. Tex., Dec. 28, 2006); *Hedenburg v. Aramark American Food Services*, 2007 U.S. Dist. LEXIS 3443 (W.D. Wash. Jan. 17, 2007); *In re Ford Motor Co.*, 345 F.3d 1315, 1316 (11th Cir. 2003); *Ameriwood v. Liberman*, 2006 WL 3825291, 2006 U.S. Dist. LEXIS 93380 (E.D. Mo., Dec. 27, 2006).

⁸¹ *Menke* supra n. 78 at 12. See also *Antico*, supra note 16 discussed below (defense made a showing of need for information on iPhone and plaintiff offered no less intrusive means for providing relevant information).

⁸² *Id.* at 10.

⁸³ *Id.* at 8.

⁸⁴ *Antico*, supra n. 16.

⁸⁵ *Antico*, supra n. 16 at 167 (“[the trial court’s order] limits the data that the expert may review to the nine-hour period immediately surrounding the accident; it gives Petitioner’s counsel a front-row seat to monitor the inspection process; and it allows Petitioner the opportunity to interpose objections before Respondents can obtain any of the data.”)

⁸⁶ *Id.*

⁸⁷ *Id.* at 168.

ITEM 9.10 | REQUESTING PRODUCTION AND MAKING PRODUCTION OF ESI

Effective September 1, 2012, the Florida Rules of Civil Procedure establish a workable framework for production of electronically stored information. The most prominent issue for production of ESI involves the form of production, which can implicate the completeness and utility of the ESI produced as well of the cost of production if the ESI must be translated or converted into the requested form. Fortunately, the rules contemplate these issues as will be discussed below. Nonetheless, the most prudent course for counsel on both sides is to confer and cooperate on the form of production beforehand to avoid disappointment, non-productive effort, and needless cost of repeated production.

A request for electronically stored information may specify the form or forms in which electronically stored information is to be produced.⁸⁸ The form should usually be specified. The requesting party should take into account the reasons for specifying a given form, such as: (1) Will the document's native functionality be needed, such as a spreadsheet's embedded calculations? (2) Will the native form⁸⁹ of the document be needed in order to determine the context in which the document was created or stored? (3) What are the format requirements of the software that the requesting party plans to use to review the production?

If the responding party objects to a requested form, or if no form is specified in the request, the responding party must state the form or forms it intends to use.⁹⁰ This is a quite sensible provision that essentially directs the parties to address any issues in the form of production. For example, if a responding party specifies a form of production and the requesting party fails to object to the form of production, the court has a meaningful record on which to determine whether production in another format will be required and which party should be required to pay the cost of the additional production. If a request for electronically stored information does not specify the form of production, the producing party must produce the information in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms, which is almost always the native format.⁹¹ Again, this is a sensible process that tells the producing party that they are not permitted to degrade or convert the electronic documents to a less useful format for production.⁹²

Example: Party A requests Party B's discoverable emails in native format. Party B's attorney dislikes using electronic forms in handling discovery and evidence, so he requests a printed copies of every one of Party B's several thousand emails and sends a copy to Party A. When Party A objects, the attorney for Party B states that he has given up every email (which, of course includes everything that would be relevant or discoverable) and "you have everything I have." Is this adequate production under the rules? Answer: No. Party B's attorney should have objected to the requested form (native) rather than producing in another form without involving Party A or the Court in the decision.⁹³ While technically every discoverable email may be included in the production, the printed out versions do not contain metadata, which may be discoverable. In addition, the printed version is not "reasonably usable" because a non-electronic version is not searchable, which can be a valuable tool with large numbers and volumes of emails. Party A, having made a proper request, is entitled to receive the emails in the form requested unless there is an objection followed by an agreement by the parties or court determination on form. In a sense, production of all the emails rather than discoverable emails can be a form of "data dump" exacerbated by the lack of ability to electronically search, sort, deduplicate, and manage the information. The dispute may have been avoided if Party B's counsel contacted Party A before going through the extra expense of providing paper copies.

The form of production may also be an issue when exercising the option to produce records in lieu of answering interrogatories, so the amendments to the civil rules effective September 1, 2012, (1) specifically authorize the production of electronically stored information in lieu of answers to interrogatories, and (2) set out the procedure for determining the form in which to produce the ESI.⁹⁴ If the records to be produced consist of electronically stored information, the records must be produced in a form or forms in which they are ordinarily maintained or in a reasonably usable form or forms.⁹⁵

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

Footnotes

⁸⁸ Fla. R. Civ. P. 1.350(b).

⁸⁹ Native format is a copy of the original electronic file. For example, e-mail from an Outlook e-mail program would be produced in a *.pst file. Native format files include the metadata of the original file. Native format files also are easy to modify. This presents difficulties in ensuring that the data has not altered after being produced. Cooperation of counsel and well-documented procedures are required to allow effective use of native format evidence at depositions and trial.

⁹⁰ Fla. R. Civ. P. 1.350(b).

⁹¹ Id. ESI is usually “ordinarily maintained” in its native format, meaning the format used by the software in which the ESI was created.

⁹² Such an effort would be equivalent to the unsavory practice of shuffling unnumbered pages or removing file labels from folders before producing paper discovery to the opponent.

⁹³ Fla. R. Civ. P. 1.350(b).

⁹⁴ Fla. R. Civ. P. 1.340(c).

⁹⁵ Id.

ITEM 9.11 | PRODUCTION OF ESI PURSUANT TO SUBPOENA

Production of electronically stored information pursuant to subpoena potentially raises the now familiar issues of form of production, undue burden, and who pays the cost of production. Fortunately, effective September 1, 2012, the civil procedure rules specifically address these issues and provide a pathway for counsel and judges to negotiate these issues.

The issue of form of production in response to a subpoena is much the same as the issues implicated in a Fla. R. Civ. P. 1.350 request for production, and amended Rule 1.410 addresses the issues in similar fashion. It makes abundant sense for the party issuing the subpoena to specify the preferred form of production. However, if a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.⁹⁶

Persons responding to a subpoena may object to discovery of ESI from sources that are not reasonably accessible because of undue costs or burden.⁹⁷ On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought or the form requested is not reasonably accessible because of undue costs or burden. Once that showing is made, the court may order that the discovery not be had or may nonetheless order discovery limited to such sources or in such forms if the requesting party shows good cause, considering the limitations set out in Fla. R. Civ. P. 1.280(d)(2). The court may specify conditions of the discovery, including ordering that some or all of the expenses of the discovery be paid by the party seeking the discovery.⁹⁸ Failure of the court or a party to make provision for cost of production from non-parties to produce subpoenaed documents is a departure from the essential requirements of the law and may remedied by certiorari review.⁹⁹ The court will undoubtedly take into account whether the subpoena is directed to a party or a person or organization controlled by or closely identified with a party, or to a person or entity totally unrelated to and disinterested in the case. Subpoenas to non-parties have become a major issue in discovery of ESI because an enormous amount of ESI is sent, stored, shared, or created on systems owned or controlled by third parties, including internet accessible sites.

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

Footnotes

⁹⁶ Fla. R. Civ. P. 1.410(c).

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *First Call Ventures, LLC v. Nationwide Relocation Servs.*, 127 So. 3d 691 (Fla. 4th DCA 2013).

ITEM 9.12 | DISCOVERY OF SOCIAL MEDIAL ESI

Social media is a term referring to a broad array of networking sites with varying participation by individuals, businesses, governmental bodies, and other organizations. Social media sites are proliferating in type, form, and content. No longer just a way for kids and young adults to connect about their current activities and status, social media has captured the attention of individuals of all ages as well as businesses, corporations, government entities, and virtually any organization or person that wants to reach target or broad audiences. Some of the more popular social media sites are Facebook, Myspace, LinkedIn, Wikipedia, Flickr, Instagram, YouTube, and Twitter, but there are many more. Social media policies, agreements, structure, make-up, and culture all differ from site to site, which creates varied and complex data management and ownership issues and significant challenges in preservation of social media content. Most social media sites include features allowing members to send direct messages between themselves, much like emails or text messages. Assuming relevancy under the facts and circumstances of a given case, social media evidence is discoverable. See *Nucci v. Target Corp.*, 162 So. 3d 146 (Fla. 4th DCA 2015).

Social media may contain important relevant evidence in any number of different legal disputes. It is important to note that the information of a member in a social media site is not obtained by subpoena of the social media provider itself, any more than email is obtained by subpoena of an email provider. The information is discovered from the member. It is their information, they own it, not the providers, and thus the proper course of conduct is a request for production, or subpoena, from them.¹⁰⁰ Text searches are run, the use of key words only determines potentially relevant documents or files. The fact that a document or file comes up in a key word search, or otherwise is found to contain an agreed upon keyword, does not in and of itself make it discoverable.

Example: Party A in a commercial case seeks discovery of all emails in the possession or control of Party B that relate to the same transaction that is at issue or similar transactions for the previous five years. Two key words selected by Party A are the word "cobalt" and the name "Prosser." Party B is willing to run those key words and then select and produce discoverable, non-privileged documents. Party A contends that it is entitled to receive all emails containing "cobalt" or

"Prosser." Is Party A entitled to the discovery of all the emails identified in the word search using these terms? Answer: NO. Relevancy is determined by examination of the document itself. The words used in a search, even if they are agreed upon by the parties as appropriate search terms, are but a tool to identify potentially relevant documents. Relevancy is determined by legal analysis of whether the document is (1) relevant to the case's subject matter, and (2) admissible in court or reasonably calculated to lead to evidence that is admissible in court.¹⁰¹ Documents that turn up in a word search may or may not meet these criteria, and Party B is only obligated to produce discoverable documents. The analog equivalent to the demand made by party A is to request a search of all file folders with the words "Cobalt" and "Prosser" on the file labels and then contend that all paper within those folders is discoverable. The determination of relevancy is made by examination of the document itself, not normally by the wording of the label on the folder in which the document is found.

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

Footnotes

¹⁰⁰ **Stored Communications Act** (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It is a waste of time to subpoena internet service providers. Instead, a social media member should be requested to produce their information, and motions to compel should be directed against them if they do not comply.

¹⁰¹ Fla. R. Civ. P. 1.280(b)(1); Balfour, *supra* n. 16.

ITEM 9.13 | CONCLUSION

Discovery of ESI is potentially complicated, ever-changing, and extremely important in many cases. Counsel must be conversant enough with the terminology, law, rules, and technology to identify issues and fully advise the client on electronic discovery issues.

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

APPENDIX

COPYRIGHT NOTICE

TextBookDiscrimination.com is not the author of this handbook. Instead, TextBookDiscrimination.com merely re-printed and reformatted them for easier use.

ORIGINAL SOURCE

<u>#</u>	<u>Item</u>	<u>Link</u>
1	Original Source	NinthCircuit.org

CONTACT INFORMATION

E: TextBookDiscrimination@gmail.com

W: www.TextBookDiscrimination.com

Congratulations! You're now **booked up** on Chapter VI from Florida's Handbook on Civil Discovery Practice (2016)!