



GUIDELINES FOR ELECTRONIC DISCOVERY, PART 1 THE FIRST 10*

By: Mary A. Prebula, Esq.
Prebula & Associates LLC
mprebula@prebulallc.com

Electronic discovery is now an issue in virtually every case, from the small breach of contract case to huge complex litigation matters. These 20 Guidelines will provide a starting point for research and use of e-discovery.

1. LEARN THE TERMINOLOGY

Sources of electronic data include computers, laptops, servers, backup media, PDAs, voicemail systems, USBs, CDs, DVDs, "thumb" drives, external hard drives, and other devices. Electronic data includes word processing files, voicemail, e-mail, deleted files, data files, program files, backup and archival files and tapes, temporary files, system history files, web site files, graphic and audio files, web log files, cache files, cookies, metadata, accounting program files, calendars, computer activity data logs, instant messaging files, cell phone texting files, browser tool bars and features (Favorites, History, and booknoted cites); and other electronically stored information ("ESI").

2. RESEARCH THE LAW

Georgia law does not currently have any express provisions with regard to electronic discovery. A few Georgia appellate cases have addressed electronic discovery issues. *See, e.g., Georgia Emission Testing Co. v. Reheis*, 268 Ga. App. 560 (2004) (affirming trial court orders allowing e-discovery and reversing splitting of costs); *WGNX, Inc. v. Gorham*, 185 Ga. App. 489 (1988) (holding computer records admissible as business records under O.C.G.A. 24-3-14); *Cotton v.*

Eshelman & Sons, Inc., 137 Ga. App. 360 (1976) (ESI admissible). For federal cases, start with *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*").

3. CONSULT WITH A COMPUTER FORENSICS EXPERT

If possible, consult with a computer forensics expert familiar with the business area of your opponent. They perform "highly specialized technical tasks to acquire, process, preserve, and track the voluminous amount of ESI . . . include[ing] forensically sound preservation of custodian computers; extraction of documents from multiple operating systems, corporate servers, and network shares while preserving meta-data; cataloging, extracting e-mail and attachments, and processing; compilation of keyword and meta-data indices for analysis and reporting . . .; auditing and logging of files and ensuring compliance with



Federal Rules; decryption and extraction of proprietary data; triage and advanced processing of files with errors; statistical and keyword analysis with related reporting; and compilation of native file production and load files to provide usable documents . . ." *CBT Flint Partners, LLC v. Return Path, Inc.*, 2009 U.S. Dist. LEXIS 121188 (N.D. Ga. 2009). In addition, counsel must identify the technology person who will answer the technical questions

and safeguard the lawyer from agreeing to some plan that will result in excessive costs and useless information.

4. DEMAND PRESERVATION OF RELEVANT ESI

Send a Preservation Letter

Ask for very broad preservation and then narrow the requested ESI through conference and your discovery requests. The duty to preserve evidence arises as soon as litigation is contemplated. *See* Bridgestone/Firestone North American Tire, LLC v. Campbell, 258 Ga. App. 767 (2002). As there are no Georgia cases directly on this topic dealing with ESI, we must all be cautious in what is preserved.

Federal law has strong preservation rules. In Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003) ("Zubulake IV") (adverse inference instruction resulting in \$29 million



verdict against the non-preserving party), the court stated that the "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation

or when a party should have known that the evidence may be relevant to future litigation."

Significantly, E-discovery where the ESI is preserved generally is much less expensive than computer forensics to recover lost data. As soon as it becomes apparent that a case may involve ESI, it is prudent to send a letter or notice requesting preservation. You can update or amend that letter once the litigation progresses such that you have sufficient knowledge to tailor the preservation hold to the case.

5. PRESERVE RELEVANT ESI EVIDENCE

Your Client Must Preserve Also

The same rules apply to your client. Make sure your client preserves all ESI that that can reasonably be anticipated without extraordinary cost. It is also significant that the duties do not stop with the letter to preserve. "A party's discovery obligations do not end with the implementation of a 'litigation hold'-to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents." Zubulake V, 229 F.R.D. at 432.

6. OBTAIN PRESERVATION ORDER IF NECESSARY

If there is any question that the opposing party will not abide by or even agree to a preservation plan, obtain a court order to preserve the data through traditional means. *See* Owens v. American Refuse Systems, Inc., 244 Ga. App. 780, 781 (2000) (a method of securing evidence is "court order directing preservation"). Request a court order that the opposing party make a complete copy of the hard drives and servers so that the data can be accessed for analysis. The order should include a provision that the party cannot alter, delete, destroy, wipe out, or use the data in any way until the copies are made.

7. RESEARCH THE OPPONENT

Check other cases. It is possible someone else has sued this client and engaged in e-discovery. That might be a source to identify systems, data devices, and shortcut the e-discovery, or even to determine where the hidden documents are.

8. SERVE e-DISCOVERY EARLY

In all likelihood, there will be some discussion and narrowing of the e-discovery. The earlier you serve the e-discovery, the better. If you can serve your e-discovery with the Complaint, it

puts the opponent on notice, helps to keep data from disappearing, and prepares the groundwork for a spoliation argument if it later becomes necessary.

9. CREATE A PRESERVATION AND RETRIEVAL PLAN

An e-discovery preservation and retrieval plan should take into consideration at least the following matters : scope of relevant ESI; capabilities for search and accessible and inaccessible data; focused search terms; data sampling to narrow the search; whether to include recovery of deleted or hidden data; method for conducting relevancy review, including who will conduct such review; relevant and non-relevant computer systems; custodians of relevant ESI; relevant time frame for preservation; cost effective method for preservation given the media in which the data is stored; format for review and production; method for identifying and handling claims of privilege or work product protected information or data, including who will conduct such review; and a method for protecting privileged data, including a "claw-back" agreement.

10. HOLD EARLY e-DISCOVERY CONFERENCE

In all cases, where electronic discovery is an issue or a potential issue, addressing the issues at the beginning of the case often avoids problems later. Unlike the federal rule, the Georgia Civil Practice Act does not require a discovery conference for the parties to meet and confer and set a discovery plan. *See* O.C.G.A. § 9-11-26; Paschal v. Prescod, 296 Ga. App. 359 (2009). The court can order such a conference but should be clear as to whether the parties are required to establish a discovery plan. *Id.*, at 361.

Failure to have such a plan can result in negative consequences for the requestor. In

Georgia Emission Testing Co. v. Reheis, 268 Ga. App. 560 (2004), the parties were unable to resolve discovery issues and the trial court entered orders regarding e-discovery and splitting of costs. On appeal, the appellate court found it was proper for the trial court to order preparation of a report on e-data because it was relevant to damages. The Court found the Plaintiff should have to bear the total cost of such production where Plaintiff plaintiff requested certain data in a report, which required the state agency defendant to hire a consultant to extract the data from a massive electronic data base, even though the data was available to the plaintiff in its own records.

Regardless of whether the case is in federal or Georgia courts, an early E-discovery conference can help create a plan to handle such discovery and narrow the discovery. FRCP Rule 26(f) mandates that counsel address E-discovery issues, and requires that counsel for all parties "meet and confer" prior to the required scheduling conference to discuss certain evidentiary issues. The outline under the rule includes: preserving relevant evidence, the disclosure and exchange of electronically stored information ("ESI"), the format in which such ESI will be produced, and the protection of materials and information protected by privilege.



*©2010. Look for Part 2 and Guidelines 11-20 in the May, 2010 GCBA Newsletter. For more expansive paper and forms, see "Electronic Discovery in Small Business Litigation", General Practice and Trial Institute, ICLE 107296 (March 11-13, 2010).