



GUIDELINES FOR ELECTRONIC DISCOVERY, PART 2 THE LAST 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. The first part of this article containing Guidelines 1-10 appeared in last month's newsletter. Guidelines 11-20 are presented here.

11. CONSIDER A SPECIAL MASTER

If the parties can agree to a special master to handle retrieval, review and screening for privilege before production is made, that will streamline the process. However, one must often decide whether the discovery dollars go toward hiring a special master to handle the E-discovery or trying to handle it with counsel and client alone.

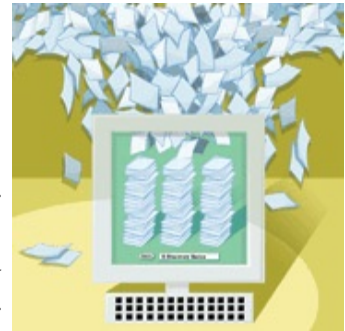
12. CAREFULLY CRAFT DISCOVERY REQUESTS

Every case is different and discovery will obviously be geared to the issues in the cases. Consider sending an initial set of requests early. Once you get responses and perhaps take some preliminary depositions, send another set crafted for the precise systems. Include such matters as computers and servers in use, operating system and any changes since events at issue in the case arose and why; system documentation; databases in use; "datamaps" or "schemas" that show how the fields relate to each other; instruction booklets and database policies and procedures; backup systems; custodians; last deletion or purge of the system

and why; deleted or trashed computers or servers and backup for deleted data; pass codes, keys and codes to obtain the data from every single system, computer, storage device if relevant to the case, e-mail addresses for relevant persons, network service providers for Internet and email, telephone, and banking facilities; and company IT personnel who best know the systems and databases.

13. BE PREPARED TO NARROW THE E-DISCOVERY AS NEEDED

Things change during the course of E-discovery. Be prepared to modify. *See Edelen v. Campbell Soup Co.*, 2009 U.S. District LEXIS 114893 (N.D. Ga. 2009) ("not unusual in the course of electronic discovery for the parties to be required to limit the scope of their requests through the use of certain key search words or terms").



14. DETERMINE WHETHER THE ESI REQUESTED IS REASONABLY ACCESSIBLE

FRCP 26(b)(2)(B) provides that a party need not provide discovery or ESI from sources identified as not reasonably accessible because of undue burden or cost. "[W]hether production of documents is unduly burdensome or expensive turns primarily on whether it is

kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of the production)." Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y 2003) ("Zubulake I").

Although this provision for accessibility is not in the Georgia Civil Practice Act, courts



in their broad discretion over discovery matters also view accessibility through possession, custody and control. See, e.g., Hammontree v. State, 283 Ga. App. 739-740 (2007)

(admitted instant messages from relative's IM account, which was not password protected where evidence party used account); Georgia Emission Testing Co. v. Reheis, 268 Ga. App. 560 (2004) (upheld trial court order requiring defendant to prepare a report that did not exist but required 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).

15. DON'T AGREE UP FRONT TO PAY COSTS FOR OPPONENT'S ESI

Until there are issues of cost and you evaluate how the court is likely to address the issue of costs, do not agree up front to pay opponent's ESI discovery costs.

16. MAKE SURE YOU GET ALL THE DATA

It is important that an exact copy be made of the data on the E-device using a write-blocking device to image the drive, which basically means that nothing is changed as it is copied. This is important, for example, to copies made from a Microsoft Windows environment because Windows automatically overwrites the date and time on each file when it is copied. If

the correct device is not used, you will not have accurate dates on the copied documents.

The copy must be made in a forensically sterile environment, essentially using proper software wiping program to make sure that all data is copied. If the wrong software is used, then the copy will not contain all data. At the same time, one can identify or flag certain files that already have been identified as relevant, such as emails, spreadsheets, encrypted files, deleted files, hidden files, and conduct key word searches to find relevant e-data.

17. MAKE SURE YOU OBTAIN ESI IN USABLE FORMAT

The format for the production of the ESI should be determined pre-production. The parties must agree if data or documents will be produced in original format and if the recipient can access such formats. If the agreement is that all material will be produced in hard copy, be sure that type of production is manageable. If the parties cannot agree, seek a court conference or intervention early.

In addition, the format in which the review will be conducted must be accessible. For example, if one produces PDF files in Word format, those documents are useless. The parties must agree whether the documents will be produced in such fashion that it is searchable. Many PDF formats are not searchable.

Another consideration is whether metadata will be produced or be accessible. Metadata is buried in documents and reveals such matters as date created, author, date last modified or saved, file name, file path, recipients, custodian. See, e.g., In re Netbank, Inc., 259 F.R.D. 656 (N.D. Ga. 2009). It also can include edits made, but not saved in the final version. Metadata can be very helpful in dating events that occurred based upon the creation and access to certain data and documents.

Courts are increasingly requiring that data be produced in native format so that all metadata is retrievable, particularly where all parties have access to the necessary software and do not come forward with a good reason why the data should not be produced in native format, or where the requestor has demonstrated a need for the metadata. *See* Ojeda-Sanchez v. Bland Farms, LLC, 2009 U.S. Dist. LEXIS 66238 (S.D. Ga. 2009); Goshawk Dedicated LTD. v. Am. Viatical Servs., LLC, 2008 U.S. Dist. LEXIS 101204 (N.D. Ga. 2008).

In certain cases, access to and production of the hard drives themselves may be ordered. *See, e.g.*, ACMG of La., Inc. v. Towers Perrin, Inc., 2007 U.S. Dist. LEXIS 91291 (N.D. Ga. 2008) (no claim of privilege and data relevant to case).

18. PROTECTION OF PRIVILEGED INFORMATION AND MATERIALS

Under Georgia law, without an agreement, the party asserting that privileged materials have been disclosed bears the burden of proving the privilege. *See, e.g.*, McKesson HBOC, Inc. v. Adler, 254 Ga. App. 500 (2002); Zielinski v. Clorox Co., 270 Ga. 38, 40 (1998). While disclosure normally would waive the privilege, inadvertent disclosure may not. *Compare, e.g.*, McKesson HBOC, Inc. v. Adler, 254 Ga. App. 500 (2002) (transmittal of attorney-client privileged documents to third party waived privilege); *with* Lazar v. Mauney, 192 F.R.D. 324 (N.D. Ga. 2000) (granting motion to strike use of document where attorney-client privilege had not been waived by inadvertent disclosure).

There does not appear to be any Georgia case on the process to follow if there is inadvertent disclosure of privileged materials. The parties can agree to a "claw-back" provision. If none is agreed upon, then the attorneys should consult the ethical rules.

FRE Rule 502(d) provides that intentional or inadvertent disclosure of privileged information does not constitute a

waiver of the attorney-client privilege for that proceeding or any other state or federal proceeding as to all parties and nonparties. The Rule allows the court to enter a non-waiver order. Rule 502(d) validates the "claw-back" provisions parties have been using in confidentiality agreements.

19. DECIDE IF DISCOVERY OF DELETED COMPUTER FILES IS RELEVANT AND WORTH THE EXPENSE

Unlike when hard copies are shredded or otherwise destroyed, when ESI is deleted, it is not gone, the deletion merely makes the space available to be overwritten with new data. There is no way to determine how much of the old document space will be overwritten or when. One might recover only part of a file depending on what has been overwritten.

20. BEWARE OF ADMISSIBILITY ISSUES

One should keep in mind admissibility as the discovery process proceeds. Once you obtain the ESI, the mission is to get it admitted into evidence. Lorraine v. Markel America Ins. Co., 241 F.R.E. 534, 537-538 (D. Md. 2007).

The law regarding admissibility of ESI in Georgia follows the normal rules of evidence. Emails and instant messages ("IMs") are "held to the same standards of authentication as other similar evidence." Simon v. State, 279 Ga. App. 844, 847 (2006) (emails admitted where identified, authenticated and evidence that party communicated through this means).

Similarly, computer printouts may be admitted under the business records exception. State v. A 24 Hour Bail Bonding, 280 Ga. App. 463, cert. den., 2006 Ga. LEXIS 794 (2006) (improperly admitted because did not meet business record exception). The witness laying the foundation for computer printouts does not have to be the person who input the data into

the computer. Reisman v. Martori, Meyer, et al., 155 Ga. App. 551, 553-554 (1980) (citing Hilliard v. Canton Wholesale Co., 151 Ga. App. 184 (1979)); Cotton v. John W. Eshelman & Sons, Inc., 137 Ga. App. 360, 363 (1976)). The backup documents for the computer printouts are not required for admissibility. Reisman, *supra*, 155 Ga. App. at 553-554. Further, summaries of computer printouts already in evidence are admissible. Reisman, *supra*, 155 Ga. App. at 553-554 (citing Eshelman, supra, 137 Ga. App. at 362; Smith v. Bank of the South, 141 Ga. App. 114 (1977)).

Federal law similarly follows the regular rules for admissibility of ESI. *See* Lorraine v. Markel America Ins. Co., 241 F.R.E. 534 (D. Md. 2007) (analysis under F.R.E. 104, 401, 403, 801-807, 901, 902, 1001-1008). *See also* United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) (noting ways ESI admissible under traditional exceptions to hearsay rule).

*©2010. Part 1 and Guidelines 1-10 appeared in the April, 2010 GCBA Newsletter. Did you miss it? You may view it here: <http://gcba.org/pdf/April%202010%20EDiscovey%20Pt%201.pdf> . For a more expansive paper and forms, see "Electronic Discovery in Small Business Litigation", General Practice and Trial Institute, ICLE 107296 (March 11-13, 2010).

CONCLUSION

While the types of matters to which discovery rules apply seem to be changing, it appears that the existing rules themselves can handle the issues unless and until new e-discovery rules are created. The key issues in all of these matters seem to be asking the right questions, narrowing the focus, controlling the cost, and managing the admissibility of what you do discover.

