

Recent Developments in Electronic Discovery

Steve Schortgen

Steve.Schortgen@BakerBotts.com
(214) 953-6826

E-Mail Can Be Painfully Candid

- **In response to a document provided by one of its authors to the CEO of a division of a multi-national company:**

"This is absolute dynamite, not at all what I expected and needs to be destroyed."

Duty to Preserve Potential Evidence

- "Preservation duty can arise before the commencement of the lawsuit, receipt of subpoena, or even the initiation of a formal investigation." Zubulake v. UBS Warburg LLC, 220 F.R.D. 216 (S.D.N.Y. 2003) ("Zubulake IV")
- "Duty to preserve 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." Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001)

Scope of Duty to Preserve

- **Preserving everything is impractical.**
- **"What is the scope of the duty to preserve? Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly 'no.' Such a rule would cripple large corporations ... that are almost always involved in litigation. As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation." Zubulake IV, 220 F.R.D. at 217.**

The *Zubulake* Rule:

- **"Anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary." Zubulake IV, 220 F.R.D. at 217**
- **"Litigants are under a duty to preserve any document it knows, or reasonably should know, 'is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.'" Id., 220 F.R.D. at 217.**

Whose Documents Must Be Retained?

- **"Documents created by or in the possession of individuals likely to have discoverable information that the disclosing party may use to support its claims or defenses. [. . .] Thus, the duty to preserve extends to those employees likely to have relevant information - the 'key players' in the case." Zubulake IV, 220 F.R.D. at 218.**
- **But how, in advance of discovery, does a company identify all the "key players?"**
 - **There is certainly no universal answer, but if someone merits inclusion in the FRCP 26 List of Persons with Knowledge, then expect opposing counsel to argue that they are "key" to the litigation.**

What Must Be Retained?

- **Once the "key players" are identified, the litigation hold should apply to all data from the relevant time period for that individual.**
- **As *Zubulake* itself recognized, this is a fact specific analysis, the answer to which depends on your particular data/network structure and topology and "litigants are free to choose how [data preservation] is accomplished." Zubulake IV, 220 F.R.D. at 218**

What Must Be Retained?

- *Zubulake* suggests, by way of example, a two step process.
- "For example, a litigant could choose to *retain all then-existing backup tapes* for the relevant personnel (if such tapes store data by the individual or the contents can be identified in good faith and through reasonable effort) and to catalog any later-created documents in a separate electronic file. That, along with a *mirror-image of the computer systems* taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents." Zubulake IV, 220 F.R.D. at 218.

Does That Mean Recycling All Data Tapes Must Cease?

- **It depends.**
- **The *Zubulake* court distinguishes two types of data for purposes of on-going data recycling efforts: (i) *accessible* and (ii) *inaccessible* data.**
- **"Accessible data" includes three categories:**
 - **Active, on-line data. *E.g.*, computer hard drive.**
 - **Near-line data. *E.g.*, optical disks and robotic data storage.**
 - **Offline storage/archives. *E.g.*, removable optical or magnetic tape media, which is generally labeled and stored on a shelf.**
 - **The main difference between near-line and off-line data is that off-line data lacks "the coordinated control of an intelligent disk subsystem." *Zubulake I*, 217 F.R.D. at 319.**

Data Types (con't)

- **"Inaccessible data" includes two categories:**
 - Backup tapes. *E.g.*, sequentially accessed tape drives.
 - Erased, fragmented or damaged data. *E.g.*, the "slack space" on a hard drive.
- **What is the real difference between the magnetic media included in the "offline storage" category and the "backup tape" category?**
 - In practice, the distinction may be largely lost.
 - The real difference appears to be whether the data needs to be restored or otherwise manipulated to be useable. If manipulation is required, then the data is deemed "inaccessible." Zubulake I, 217 F.R.D. at 319-20.

Data Type Matters Because . . .

- ***Zubulake IV* states that "the litigation hold does *not* apply to inaccessible back-up tapes (*e.g.*, those maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy."**
- **"On the other hand, if backup tapes are accessible (*e.g.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold."**
- **But, if the company can identify where particular employee documents are stored on backup tapes, the tapes storing the documents of the "key players" must be preserved whether the data is accessible or inaccessible. Zubulake IV, 220 F.R.D. at 218**

Zubulake In Action

"What we've got here is a failure to communicate."

What Counsel did:

- 1. in-house counsel gave oral instructions to preserve documents (but didn't address backup tapes);**
- 2. outside counsel met with a number of key players in the litigation and reiterated in-house counsel's instructions, specifically referencing e-mail;**
- 3. in-house counsel followed up, reducing the litigation hold instructions to writing and sending via e-mail; and**
- 4. after receiving a specific document request for e-mail on backup tapes, outside counsel requested UBS's IT personnel to stop recycling backup tapes.**

Counsel's Duty to Locate Relevant Information

- Referring back to *Zubulake IV*, Judge Scheindlin summarized a litigant's preservation obligations and identified steps that counsel should take to ensure compliance with a preservation obligation.
- 1. Counsel must issue a "litigation hold" when litigation is reasonably anticipated. The hold should be periodically re-issued to keep it "fresh in the minds of all employees."
- 2. Counsel should communicate directly with the "key players" and communicate the preservation duty clearly.

Counsel's Duty to Locate Relevant Information (Cont'd)

- 3. "Counsel should instruct all employees to produce electronic copies of their relevant active files." This will likely require an interview and questioning on the witnesses' "document management habits."**
- 4. Counsel must make sure that all backup tapes which the party is required to retain are identified and stored in a safe place. This will require meeting with IT personnel and learning the system.**

Traditional Methods May Not Suffice

- The traditional method of establishing the litigation hold may not be enough.
- "In short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take *affirmative steps* to monitor compliance so that all sources of discoverable information are identified and searched." Zubulake V, 2004 WL 1620866
- The additional step of *monitoring compliance* may be new to some companies.
 - "A party cannot reasonably be trusted to receive the 'litigation hold' instruction once and to fully comply with it without the active supervision of counsel." *Id.*

What Counsel Didn't Do In *Zubulake*

- 1. One key witness testified at deposition that while she was instructed to retain her files, she was never asked to produce them.**
- 2. One key witness testified she had an "archive file" on her computer pertaining to the Plaintiff. Outside counsel apparently misunderstood the statement and believed it referred to backup tapes rather than an archive on the witnesses' computer and did not properly follow up.**

What Counsel Didn't Do (Cont'd)

- 3. Both inside and outside counsel failed to communicate with a key HR witness.**
- 4. Counsel failed to protect backup tapes, resulting in key tapes being lost or overwritten.**
- 5. Counsel failed to "ascertain each of the key players' document management habits."**

Remedy

- 1. Adverse inference instruction.**
- 2. UBS to pay costs for depositions or re-depositions required by late production of data.**
- 3. UBS to pay costs of motion.**

Best Practices - The Sedona Guidelines

- **What is the Sedona Conference?**
 - *Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* was issued for public comment in September 2004.
- **Do the guidelines present a safe harbor?**
 - Not expressly, but they do present a reasoned and neutral set of retention boundaries to which companies may appeal.
- **The guidelines recognize that each company's document retention strategy will be unique to that organization. Further, there may be significant variances even *within* a single entity.**
 - *E.g.*, documents related to regulatory matters may require different treatment than mundane HR issues.

Best Practices - The Sedona Guidelines

- **Start by creating a matrix of the externally mandated laws and regulations that govern the company.**
 - **FDA**
 - **IRS**
 - **SEC/SarbOx**
 - **Department of Labor**
 - **EEOC**
 - **EPA**
 - **Department of Defense**
 - **FTC (antitrust and M&A activities)**
- **It is likely that the matrix will result in differing treatment for various classes of data.**

Best Practices - The Sedona Guidelines

- **Is this a swamp? Where's the bedrock?**
- **The bedrock will shift even within a company. The Guidelines repeatedly emphasize that a one-size fits all solution simply does not exist.**
- **The Guidelines are, however, realistic:**
 - **Comment 3.a -- Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.**
 - **Comment 3.b -- Systematic deletion of electronic information is not synonymous with evidence spoliation.**

Best Practices - The Sedona Guidelines

- **For example, the Eighth Circuit stated that whether deletion of electronic evidence is tantamount to spoliation requires a three part analysis:**
 - **whether the document management records policy is reasonable considering the facts and circumstances surrounding the relevant documents;**
 - **whether the policy was adopted in bad faith; and**
 - **whether lawsuits have been filed or complaints made in the past with such frequency or in such magnitude that it is obvious that certain categories of documents should be retained.**
- **Levy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988)**

Best Practices - The Sedona Guidelines

- **Can data responsive to each matrix item be isolated at a technical level?**
 - **Consider whether the company can restructure its data/network architecture to facilitate disparate treatment of data types.**
 - **If so, retention is easier to accommodate and the risk of data slipping through the cracks is minimized.**
 - **Data segregation also more readily permits a company to adopt differing retention policies based upon data type or business unit.**

Best Practices - The Sedona Guidelines

- **Require employees to archive email on the server side (and not in individual .pst files on their hard drives).**
 - **This helps maintain data integrity in accordance with the company's stated data policy.**
- **Consider whether the utility of instant messaging is outweighed by the data preservation obligations suggested by the matrix.**
- **Do senior leaders have access to company provided PDAs or cell phones that may contain relevant data?**
 - **If so, confirm that calendars and other significant data is synced to the desktop and backed-up as appropriate.**
- **Document the steps taken to implement the litigation hold.**

Best Practices - The Sedona Guidelines

- **Designate a "technology custodian" who oversees data retention and can quickly (and without ambiguity) implement appropriate litigation holds. The custodian must be reasonably fluent in IT "geek speak."**
- **Consider whether the company's retention matrix suggests that *meta-data* - for limited classes of data - should be retained.**
 - **Few documents, however, are draft or version-centric.**
- **Carefully consider the impact of email "janitor" programs.**
 - **These programs automatically delete emails meeting certain criteria. Outlook has its own built-in janitor feature; other companies use commercial software for this purpose.**

Best Practices - The Sedona Guidelines

- **Be mindful of obligations created by SarbOx and related law:**
 - *E.g.*, Sarbanes §103(a)(2)(A)(i) mandates that audit work papers and other information related to any audit report be maintained by the auditors for a period of not less than 7 years. Many auditors are passing that obligation on to their clients.
- **Systematic employee education helps set the context for later litigation disagreements.**
- **Conduct periodic compliance audits.**
- **When confronted with onerous requests for electronic evidence, offer to sample data first to gauge responsiveness and relevance.**

Best Practices - The Sedona Guidelines

- **Finally, Sedona guideline Appendix C contains a helpful survey that begins to outline the appropriate elements to consider in revising a data retention policy.**
- **Presently, there are numerous proposed amendments to the Federal Rules of Procedure many of which relate to electronic discovery.**

Recent Developments in Electronic Discovery

Steve Schortgen

Steve.Schortgen@BakerBotts.com
(214) 953-6826